1/2019

DVD Deutsche Vereinigung für Datenschutz e.V.

Datenschutz Nachrichten

42. Jahrgang
ISSN 0137-7767
12,00 Euro



■ Verantwortlichkeiten bei Social-Media-Plattformen ■ Der Prominentenhack und Lehren daraus ■ beyond-EVE – Eine alternative Social-Media-Plattform ■ Twitter und Datenschutz ■ Messenger – Eine kleine Orientierungshilfe ■ Presserklärungen ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



Mittwoch, 01. Mai 2019
Redaktionsschluss DANA 2/2019
Ein Jahr DS-GVO – ein Résumé

Mittwoch, 05. Juni 2019 – Donnerstag, 06. Juni 2019
BvD-Verbandstage 2019
Künstliche Intelligenz und die DS-GVO – (k)ein Konflikt?
Berlin

Samstag, 08. Juni 2019
BigBrotherAwards 2019
Bielefeld

Samstag, 22. Juni 2019,
DVD-Vorstandssitzung
Bielefeld

Foto: Pixabay..com

DANA

Datenschutz Nachrichten

ISSN 0137-7767

42. Jahrgang, Heft 1

Herausgeber

Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)

Heinz Alenfelder
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz

Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck

Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0) 91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis

Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe

Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos

Frans Jozef Valenta, Pixabay, AdobeStock, Wikipedia

Editorial



Social-Media – Verweigern, gestalten oder Alternativen suchen?

Sie kennen die typischen Antworten zum Thema Social-Media, sei es nun das verneinende „Mit Twitter kenne ich mich überhaupt nicht aus“ oder das zähneknirschend akzeptierende „Klar kenne ich die Datenschutzprobleme mit WhatsApp – ich habe auch nur eine Gruppe mit meiner Familie und Freunden“. Die meisten Befragten haben zu vielen sozialen Medien eine persönliche Position eingenommen, die sehr oft auf das Privacy Paradoxon hinausläuft. Viele Kritikpunkte werden angeführt, doch sich völlig abstinent zu verhalten heißt oft von dem sozialen Geschehen ausgeschlossen zu sein.

Mit den Beiträgen in diesem Heft gehen wir der Verantwortung der Betreiber auf den Grund, analysieren erstmalig in der DANA das Phänomen Twitter und zeigen Alternativen auf zu Facebook und WhatsApp. Angesichts der Größe des Skandals um fast 1000 gehackte Prominenten-Accounts sahen wir uns außerdem veranlasst, diesen komplett zu dokumentieren.

Und seit Januar ist Ulrich Kelber Bundesbeauftragter für Datenschutz und Informationsfreiheit. Roland Appel verabschiedet sich mit seinem Artikel von der nun ehemaligen BfDI, Frau Voßhoff.

Die Nachrichten aus dem In- und Ausland runden das Heft wie immer ab. Außerdem liegt dieser DANA das Register für das vergangene Jahr 2018 bei.

Wir wünschen Ihnen eine gute Lektüre!
Heinz Alenfelder

Autorinnen und Autoren dieser Ausgabe:

Heinz Alenfelder
Vorstandsmitglied in der DVD,
alenfelder@datenschutzverein.de, Köln

Roland Appel
Unternehmensberater und Publizist,
roland.appel@roaconsult.com, Bornheim

Katrin Lowitz
Architektin, Ingenieurin, Gründerin von www.beyond-EVE.com,
info@beyond-eve.com

Klaus-Jürgen Roth
dvd@datenschutzverein.de

Frans Valenta
Vorstandsmitglied in der DVD,
valenta@datenschutzverein.de, Bonn

Dr. Thilo Weichert
Vorstandsmitglied in der DVD, Netzwerk Datenschutzexpertise,
weichert@datenschutzverein.de, Kiel

Thilo Weichert

Verantwortlichkeiten bei Social-Media-Plattformen

1 Vorgeschichte

Seit 2011 kämpft das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) dafür, dass Betreiber von Seiten auf Social-Media-Plattformen dafür sorgen müssen, dass der Datenverkehr, der über die Nutzung der eigenen Seite ausgelöst wird, auch beim Plattformbetreiber datenschutzkonform ist. Die Frage der Verantwortlichkeit für die Social-Media-Datenverarbeitung stellt sich angesichts der dort praktizierten **Komplexität und Arbeitsteilung** bei praktisch allen Anwendungen: der Suche, der Werbung, der Individual- und Gruppenkommunikation, dem Bloggen, dem Einsatz von Apps und Plug-ins, dem Online-Handel oder dem Online-Zahlen.

Konkret ging es bei den Verfahren des ULD insbesondere um den Betrieb von **Facebook-Fanpages**. Dieser war damals und ist bis heute datenschutzrechtlich unzulässig.[1] Zumindest bei kommerziell Nutzenden kommt den Plattform-Nutzenden eine (Mit-)Verantwortlichkeit für die Rechtmäßigkeit der Datenverarbeitung durch die Plattform zu. Da das ULD die Auswertung der Daten aus der Fanpagenutzung bei Facebook für unzulässig ansah, beanstandete es den Betrieb vieler privater und öffentlicher Fanpages. Einige wenige öffentliche Stellen machten daraufhin ihre Fanpage dicht, die meisten nicht.

Für die kommerziellen Anbieter von Fanpages warf sich die Industrie- und Handelskammer Schleswig-Holstein (IHK) mit Vehemenz in die Bresche: Es gehe doch nicht an, dass den Unternehmen in Schleswig-Holstein das **verboten werde, was weltweit praktiziert** wird – nämlich die Werbung für sich und die Vermarktung über eine Facebook-Fanpage. Dies sei geschäfts- und standortgefährdend. Selbst der Ministerpräsident des Landes Schleswig-Holstein, Torsten Albig, weigerte sich, seine Seite dicht zu machen. Dies fand Fürsprache vieler „Realisten" in der Rechtswissenschaft. So nahm z. B. das Lorenz-von-Stein-Institut der Christian-Albrechts-Universität zu Kiel unter der Leitung von Utz Schliesky, zugleich CDU-Landtagsdirektor, mit einer pseudowissenschaftlichen Publikation Partei für die Facebook-Fanpagebetreiber, von der IHK bis zum Ministerpräsidenten.[2]

Das ULD ließ sich auf einen Deal ein. Es verzichtete nicht nur auf die sofortige Vollstreckbarkeit des Betriebsverbots der Fanpages durch die privaten Unternehmen, sondern verständigte sich mit der IHK darauf, im Hauptsacheverfahren einen **Musterprozess** wegen des Fanpage-Betriebs gegen die IHK-Tochter Wirtschaftsakademie Schleswig-Holstein zu führen und bis zu dessen Abschluss die aufsichtsbehördlichen Füße in dieser Frage still zu halten.[3]

Damit begann Ende 2011 eine Prozessodyssee, die bis heute nicht abgeschlossen ist. Die erste Instanz, das Verwaltungsgericht (VG) Schleswig, zeigte nach über eineinhalb Jahren Brüten überhaupt kein Verständnis für das ULD und dessen Argumentation, dass kommerzielle Werbung über Social Media bei ausländischen Betreibern wie Facebook datenschutzkonform sein müsse.[4] Die Hoffnung, dass die Berufungsinstanz des Oberverwaltungsgerichts (OVG) in Schleswig grundrechtsorientierter entscheiden würde, wurde ein weiteres Jahr später enttäuscht.[5]

Das ULD legte gegen dieses Berufungsurteil Revision ein.[6] Erst jetzt begann langsam eine **juristische Debatte**, bei der zumindest teilweise die Überlegungen des ULD ernsthaft erwogen wurden[7]: Es kann nicht angehen, dass man sich durch die Nutzung eines Portals seiner datenschutzrechtlichen Verantwortung entledigt. Das Problem besteht nicht nur für Facebook, sondern praktisch für alle Social Media, nach deutscher Terminologie also für alle Telemediendienste (§ 1 Abs. 1 TMG), die ihrerseits wieder Webseiten und andere Mediendienste einbinden. Das ULD hatte von Anfang an damit argumentiert, dass auch bei einer Auftragsdatenverarbeitung durch Einschaltung sonstiger IT-Dienstleistenden – damals nach § 11 BDSG-alt – kein Abschieben der Verantwortlichkeit möglich ist.

Das als Revisionsinstanz angerufene **Bundesverwaltungsgericht** (BVerwG) verharrte ebenso wie die Vorgerichte in der überkommenen, begriffsorientierten Datenschutzdenke. Doch erkannte es eine Schutzlücke, weshalb es den Europäischen Gerichtshof (EuGH) anrief.[8] Der Schlussantrag des EuGH-Generalanwalts, Bot, vom 24.10.2017 übernahm dann fast vollständig die Argumentation des ULD.[9] Und dieser Position schloss sich dann mit Urteil vom 05.06.2018 auch der EuGH an, wenige Tage nachdem die Europäische Datenschutz-Grundverordnung (DSGVO) direkt anwendbar geworden war.[10] Das Verfahren hängt nun wieder beim BVerwG. Sollte das BVerwG erneuten Beweisbedarf sehen, so dürfte es das konkrete Verfahren wieder zurück an das OVG Schleswig verweisen. Es ist nicht absehbar, wann also das konkrete Verfahren der Wirtschaftsakademie der IHK Schleswig-Holstein abgeschlossen sein wird. Doch darauf kommt es nicht mehr an. Der EuGH hat die Rechtsfragen zur Verantwortlichkeit bei Social Media geklärt.

2 Verfahren beim EuGH

Rechtlicher Anknüpfungspunkt der datenschutzrechtlichen Verantwortlichkeit ist, so der EuGH, dass eine Stelle „allein oder gemeinsam mit anderen über die **Zwecke und Mittel** der Verarbeitung von personenbezogenen Daten entscheidet".[11] Bei der Antwort auf die Frage, wann dies der Fall ist, lässt sich das oberste europäische Gericht vom Ziel leiten, „einen wirksamen und umfassenden Schutz der betroffenen Personen zu gewährleisten".[12]

Es stellt fest, dass mit der Einrichtung einer Fanpage ein **Vertrag** zwischen dem Fanpagebetreiber und dem Plattformbetreiber Facebook entsteht,

dessen Inhalt durch Nutzungsbedingungen „einschließlich der entsprechenden Cookie-Richtlinie“ von Facebook vorgegeben ist.[13] Im Rahmen des durch Einrichtung der Fanpage zustande kommenden Vertrags wird Facebook eine umfassende Nutzung der Betroffenendaten ermöglicht und die Platzierung von Cookies auf den Geräten der Endnutzenden vorgesehen: „Folglich trägt der Betreiber einer auf Facebook unterhaltenen Fanpage zur Verarbeitung der personenbezogenen Daten der Besucher seiner Seite bei.“[14] Er ermöglicht dadurch ein umfassendes Profiling der BesucherInnen, dessen Ergebnisse auf Seite der Fanpagebetreiber anonymisiert mitgeteilt werden, auf Seiten von Facebook aber personenbezogen bleiben. Das Datenschutzrecht verlange nicht, „dass bei einer gemeinsamen Verantwortlichkeit mehrerer Betreiber für dieselbe Verarbeitung jeder Zugang zu den betreffenden personenbezogenen Daten hat“.[15] Der Fanpagebetreiber ist also „an der Entscheidung über die Zwecke und Mittel der Verarbeitung … beteiligt“ und damit gemeinsam mit Facebook verantwortlich.[16]

Dass die Ziele des Fanpagebetreibers nicht völlig mit denen von Facebook übereinstimmen, kann ihn nicht von seinen Pflichten befreien.[17] Die von den gemeinsam Verantwortlichen verfolgten **Zwecke können unterschiedlich sein**; sie können sich ergänzen und dürfen sich faktisch nicht gegenseitig ausschließen. Dies gilt insbesondere auch, wenn die BesucherInnen als Betroffene keine Nutzenden mit Facebook-Benutzerkonto sind.[18]

Abschließend wird vom EuGH klargestellt, dass die Bewertung „nicht zwangsläufig eine gleichwertige Verantwortlichkeit der verschiedenen Akteure zur Folge hat, die von einer Verarbeitung personenbezogener Daten betroffen sind. Vielmehr können diese Akteure in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß in der Weise einbezogen sein, dass der **Grad der Verantwortlichkeit** eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist.“[19] Damit wird ErwGr. 79 DSGVO bekräftigt, wonach es auch bei der gemeinsamen Verantwortlichkeit „einer klaren Zuteilung der Verantwortlichkeiten“ bedarf.

Die Frage gemeinsamer Verantwortlichkeit steht inzwischen im Fokus datenschutzrechtlicher Diskussionen. Dies ist mit der hohen praktischen Relevanz begründet. Viele rechtliche und praktische Folgefragen müssen beantwortet werden. Für diese Antworten bieten weitere EuGH-Verfahren einiges Material. So entschied der EuGH kurz nach seinem Facebook-Urteil und jenseits der Debatte zu Social Media zur gemeinsamen Verantwortlichkeit der Zeugen Jehovas und der für diese tätigen von Tür zu Tür verkündenden und Daten sammelnden Missionare. Auch hier bejahte der EuGH die gemeinsame Verantwortung und, dass dies „nicht zwangsläufig eine gleichwertige Verantwortlichkeit der verschiedenen Akteure für dieselbe Verarbeitung personenbezogener Daten zur Folge“ hat: „Vielmehr können diese Akteure in die Verarbeitung personenbezogener Daten **in verschiedenen Phasen und in unterschiedlichem Ausmaß** einbezogen sein, so dass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist“.[20] Im vorliegenden Fall ergab sich eine Differenzierung dadurch, dass die konkreten Erhebungsprozesse ausschließlich von den Verkündigenden, die generelle Verarbeitungsstrategie durch Koordination und Organisation sowie die anschließende Zusammenführung und Weiterverarbeitung aber gemeinsam bzw. durch die Vereinigung bestimmt wurden.[21]

Die gemeinsame „Entscheidung über die Zwecke und Mittel der Verarbeitung“ beurteilt sich **objektiv** und nicht danach, dass dies „mittels schriftlichen Anleitungen oder Anweisungen … erfolgen muss“.[22] „Eine natürliche oder juristische Person, die aus Eigeninteresse auf die Verarbeitung personenbezogener Daten Einfluss nimmt und damit an der Entscheidung über die Zwecke und Mittel dieser Verarbeitung mitwirkt“, kann als für die Verarbeitung Verantwortlicher angesehen werden.[23]

Die nächste EuGH-Entscheidung zum Thema ist nach einer Vorlage des OLG Düsseldorf[24] zu erwarten zur Verantwortlichkeit des Betreibers einer Webseite, der dort ein von einem Dritten bereitgestelltes Plugin, nämlich den **Facebook-„Gefällt mir“-Button**, eingebunden hat. Gemäß der Ansicht des diese EuGH-Entscheidung vorbereitenden Generalanwalts, Bobek, sind der Webseitenbetreiber und Facebook als gemeinsame Verantwortliche anzusehen, wobei sich die gemeinsame Verantwortlichkeit des Webseitenbetreibers auf die Verarbeitungsvorgänge beschränkt, „für die er tatsächlich einen Beitrag zur Entscheidung über die Mittel und Zwecke der Verarbeitung der personenbezogenen Daten leistet.“ Sie bestehe nicht, wenn der Webseitenbetreiber weder für die vorhergehenden noch die nachfolgenden Phasen der Gesamtkette der Datenverarbeitungsvorgänge verantwortlich gemacht werden (kann), für die er weder die Zwecke noch die Mittel habe festlegen können.

Gemeinsame Verantwortlichkeit bestehe also beim „Gefällt-mir“-Button nur für die **„Phase der Erhebung und Übermittlung.“** Trotz fehlender Zweckidentität bestehe eine Einheit der Zwecke: Es würden kommerzielle und Werbezwecke verfolgt. Die Entscheidung der betroffenen Webseiten-Betreiberin, der FashionID, den Facebook-„Gefällt mir“-Button auf ihrer Webseite einzubinden, scheine von dem Wunsch getragen gewesen zu sein, die Sichtbarkeit ihrer Produkte über das soziale Netzwerk zu erhöhen. Die materiellrechtliche Zulässigkeit, für die auch der Webseiten-Betreiber zur Rechenschaft gezogen werden kann, sei dann eine Frage der Abwägung zwischen den berechtigten Interessen der Verantwortlichen und den schutzwürdigen Betroffeneninteressen (vgl. Art. 6 Abs. 1 S. 1 lit. f DSGVO).[25] Es ist damit zu rechnen, dass – wie auch bei den beiden vorangegangenen Verfahren – der EuGH hier dem Votum des Generalanwalts folgen wird, so dass diese Positionen als geklärt angesehen werden können.

Es kann also zusammengefasst werden, dass eine gemeinsame Verantwortlichkeit bei allen Formen **kumulativen Zusammenwirkens** gegeben ist. Davon kann immer ausgegangen werden, wenn die Datenverarbeitung ohne den direkten Input der Stelle potenziell anders gestaltet worden wäre. Bereits die Veranlassung wie auch eine direktive

Mitgestaltung sind verantwortungsbegründend. Dies gilt z. B. auch, wenn bei einer Auftragsverarbeitung der Auftragnehmer über seine klassische weisungsabhängige Unterstützungsfunktion hinaus tätig wird (Art. 28 Abs. 10 DSGVO).[26] Relevant ist nicht die (getrennte) Betrachtung der einzelnen Verarbeitungen (Mikroebene), sondern die Beurteilung der Verarbeitungsschritte aus der Sicht der Betroffenen (Makroebene). Einheitliche Verarbeitungen und zwangsläufige Verarbeitungsketten begründen eine gemeinsame Verantwortlichkeit.[27]

3 Nutzerdatenverarbeitung und Datendrittbezug

Weitgehend ungeklärt blieb bisher die rechtliche Frage, inwieweit auch **Nutzende** von Social-Media-Plattformen als datenschutzrechtlich Verantwortliche anzusehen sind. Dies gilt zwar nicht für die eigenen Daten, da die Nutzenden insofern ausschließlich Betroffene i. S. v. Art. 4 Nr. 1 DSGVO sind. Zugleich aber werden bei der Nutzung von Plattformen wie Facebook die Daten Dritter an den Plattformbetreiber übermittelt, etwa in Form der Adressbücher, selbst wenn diese Dritte nicht Mitglieder der Plattform sind. Eindeutig ist die Verantwortlichkeit des Nutzenden, wenn er über Social Media Inhalte über Dritte ins Netz stellt.[28]

Das Gesetz gibt auf die Frage, wie **Daten aus Social Media mit Drittbezug** geschützt werden, keine explizite Antwort. Nach Abschluss der Kommunikation mit einem Kommunikationspartner befinden sich die Absenderdaten umfassend in der Verfügungsmacht des Empfängers;[29] dies bedingt für den Empfänger Befugnis und Bürde zugleich. Die betroffenen Empfänger müssen mit den Daten der Dritten pfleglich umgehen. Bei der Internetkommunikation wird den Kommunikationspartnern die Wahrnehmung ihrer Verantwortung oft dadurch von den Plattformanbietern unmöglich gemacht, dass diese die Adress- und Sendedaten der anderen Kommunikationspartner ungefragt z. B. zu Profilingzwecken abziehen. Dies entbindet die Empfangenden aber nicht von ihrer Pflicht und Verantwortlichkeit. Sie dürfen (eigentlich) keine Verfahren nutzen, über welche Drittdaten entsprechend unkontrolliert abgezogen und genutzt werden.

Die Plattformnutzenden bestimmen über die „Zwecke und Mittel der Verarbeitung" durch die Auswahl der Plattform mit. Bezüglich jeder Form von Daten mit Drittbezug bedeutet dies, dass die Person, deren Daten verarbeitet werden, für die Rechtmäßigkeit der Datenverarbeitung der durch den Drittbezug Betroffenen **(mit) verantwortlich** ist. Die (Mit-)Verantwortlichkeit der in erster Linie „betroffenen Person" entbindet selbstverständlich nicht den Plattformbetreiber von der Beachtung des Datenschutzrechts auch in Bezug auf Dritte. Bei Drittbezug entsteht also die – nur auf den ersten Blick – ungewöhnlich erscheinende Situation, dass ein Betroffener und weitere verarbeitende Stellen gemeinsam nach Art. 26 DSGVO verantwortlich sein können.

Der Drittbezug von personenbezogenen Daten schließt nicht aus, dass der Betroffene darüber verfügt. Der Betroffene hat, weil es auch „seine Daten" sind, hieran grds. ein **„berechtigtes Interesse"** (Art. 6 Abs. 1 S. 1 lit. f DSGVO). Wohl aber ist er als Verantwortlicher verpflichtet darauf zu achten, dass dabei nicht „die Interessen oder Grundrechte und Grundfreiheiten" der betroffenen Dritten überwiegen. Der Plattformanbieter muss also den Nutzenden durch entsprechende Zusicherungen gewährleisten, dass die Interessen der Dritten nicht beeinträchtigt werden. Fehlt es hieran, so dürfen – streng nach dem Datenschutzrecht – UserInnen die jeweilige Plattform nicht verwenden, soweit bei ihrer Nutzung Drittdaten anfallen.

Verantwortlichkeit setzt **Identifizierbarkeit** voraus. D. h. Internetnutzende müssen zur Verantwortung für ihr Handeln im Netz gezogen und dafür identifiziert werden können, wenn Daten von Dritten verarbeitet werden. Dies bedeutet nicht, dass im Interesse der Datensparsamkeit auf die Möglichkeit der pseudonymen Netznutzung verzichtet werden muss. Wohl aber sind dann Prozesse nötig, mit denen bei Drittdatenverarbeitung pseudonyme Nutzende (re-)identifiziert werden können. Dies steht nicht im Widerspruch zu der Regelung des § 13 Abs. 6 Telemediengesetz (TMG), der „soweit technisch möglich und zumutbar" einen Anspruch auf Nutzung „anonym oder unter Pseudonym" begründet.[30] Bei gemeinsamer Verarbeitung mit Drittbezug kommt eine anonyme Nutzung nur in Ausnahmefällen in Betracht, wenn der Drittschutz etwa durch Rechtsschutzmöglichkeiten der Dritten bei einem anderen (gemeinsam) Verantwortlichen gesichert ist; die pseudonyme Nutzung legt grds. einen Prozess der Reidentifizierung im (Dritt-) Betroffeneninteresse nahe.

4 Vereinbarung

Welche Folgen hat die gemeinsame Verantwortlichkeit bei Social-Media-Plattformen? Die Antwort darauf gibt **Art. 26 DSGVO**: Die gemeinsam Verantwortlichen „legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß der Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind" (Art. 26 Abs. 1 S. 2 DSGVO). Die Vereinbarung muss gemäß Art. 26 Abs. 2 DSGVO „die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln", was bedeutet, dass diese den Betroffenen zumindest auf Nachfrage zur Verfügung zu stellen ist. Adressat der Wahrnehmung der Betroffenenrechte sind sämtliche gemeinsam Verantwortlichen (Abs. 3).

Die gemeinsam Verantwortlichen werden zum Abschluss einer Vereinbarung, also eines Vertrags, verpflichtet.[31] Die Regelung geht davon aus, dass grds. kein Über-Unterordnungsverhältnis zwischen den Vertragspartnern besteht, sondern eine gleichberechtigte **Verantwortung im Sinne einer Arbeitsteilung.**[32] Eine stillschweigende Kooperation von Stellen mit einer konkludenten „Vereinbarung" ist praktisch ausgeschlossen.[33] Anders als für die Auftragsverarbeitung (Art. 28 Abs. 9 DSGVO) ist aber keine bestimmte Form vorgesehen.[34]

Die Vereinbarung muss „die jeweiligen **tatsächlichen Funktionen und Beziehungen** der gemeinsamen Verantwortlichen gegenüber den Betroffenen gebührend widerspiegeln" (Art. 26 Abs. 2 S. 1 DSGVO). Dies hat denklogisch zur Folge, dass die Vereinbarung auch die Beziehung zwischen den gemeinsamen Verantwortlichen regelt: Die Darstellung hinsichtlich der Rechte und Pflichten gegenüber den Betroffenen grenzt zugleich die Pflichten untereinander im Innenverhältnis ab.[35] Die Pflicht zur Vereinbarung hat vorrangig die Funktion der Wahrung der Betroffenenrechte, wozu auch das Recht gehört, dass die eigenen Daten rechtmäßig verarbeitet werden.[36] Zugleich wird damit aber auch das Rechtsschutzinteresse zwischen den Verantwortlichen gewahrt.[37] Es soll ausgeschlossen werden, dass im Fall eines Ungleichgewichts zwischen den „Verantwortlichen eine ungebührliche interne ‚Freizeichnung' eines Verantwortlichen vereinbart wird".[38] Die Verteilung der Verantwortlichkeiten gemäß der Vereinbarung muss den faktischen Verhältnissen folgen und kann eine interne Aufgabenaufteilung zwischen den Verantwortlichkeiten regeln.[39]

Durch die private Vereinbarung kann das **staatlich vorgegebene Recht nicht modifiziert** werden. D. h. die Rechte und Pflichten der DSGVO bzw. generell der Datenschutzgesetze gelten und zwar für jeden der Verantwortlichen.

In Art. 26 DSGVO werden die in der Vereinbarung **nötigen Inhalte** benannt, nicht aber deren Detailliertheitsgrad.[40] Wesentlich sind alle Inhalte, die den Umgang mit den personenbezogenen Daten betreffen und die diesbezügliche Organisation der Verantwortlichen.[41] Da die Vereinbarung nicht nur im Innen-, sondern auch im Außenverhältnis, also auch gegenüber den Betroffenen, Transparenz (Art. 5 Abs. 1 lit. a DSGVO) schaffen soll, müssen die Anforderungen der Art. 13, 14 DSGVO erfüllt sein, wozu gehört, dass die Angaben für die Betroffenen präzise, leicht zugänglich, verständlich und in klarer Sprache gefasst sein müssen (Art. 12 Abs. 1, 26 Abs. 2 S. 2 DSGVO).[42]

Zentraler **Inhalt der Vereinbarung** muss es sein, die Zwecke und Mittel der Datenverarbeitung der jeweiligen Verantwortlichen zu benennen.[43] Weitere obligatorische Inhalte ergeben sich durch die in den Art. 13, 14 DSGVO aufgeführten Informations- und die in Art. 15 DSGVO dargelegten Auskunftspflichten.[44] Die Verantwortlichen müssen sich gegenseitig die Informationen zur Verfügung stellen, die zur Erfüllung der Informationspflichten benötigt werden.[45]

Selbstverständlich muss die Datenverarbeitung sämtlicher gemeinsam Verantwortlicher rechtmäßig sein. Soweit die gemeinsame Verantwortlichkeit reicht, müssen die Voraussetzungen der Rechtmäßigkeit bei allen Verantwortlichen vorliegen. Erfolgt z. B. ein Tracking durch einen der gemeinsam Verantwortlichen, so wie dies bei den Fanpages, dem Like-Button oder beim Custom Audience von Facebook der Fall ist, dann bedarf es grds. der Einwilligung der Nutzenden.[46] Um die **Rechtmäßigkeit beurteilen** zu können, müssen sich die gemeinsam Verantwortlichen gegenseitig über die relevanten Informationen hierzu austauschen.[47]

Hinsichtlich datenschutzrechtlich relevanter Vertragsinhalte von Datenverarbeitern ist Art. 28 DSGVO zur Auftragsverarbeitung und dort insbesondere der Absatz 3 stilbildend. Bei den notwendigen Regelungspunkten kann insofern eine Anleihe gemacht werden, wobei aber die anders gelagerte Beziehung zwischen den Vertragspartnern berücksichtigt werden muss: Während beim Auftrag zumindest formal ein Über-Unterordnungsverhältnis besteht, haben wir hier – auch zumindest formal – eine gleichberechtigte Beziehung. Bei der Auftragsdatenverarbeitung hat der Auftraggeber die vorrangige materiell-rechtliche Verantwortung; bei der gemeinsamen Verantwortung liegt diese bei allen Verantwortlichen uneingeschränkt. Entsprechendes gilt für die Voreinstellungen (Privacy by Default) gemäß Art. 25 Abs. 2 DSGVO. Hinsichtlich der sonstigen technisch-organisatorischen Vorkehrungen nach Art. 32 DSGVO, die bei der Auftragsverarbeitung voll dem Auftraggeber zugeordnet bleiben, können und müssen dagegen bei gemeinsamer Verantwortlichkeit dort Abstriche gemacht werden, wo der jeweilige Verantwortliche arbeitsteilig die „Verantwortung" übernimmt. Anders als beim materiellen Recht und beim Privacy by Default gibt es hier nicht nur richtige oder falsche Lösungen. Vielmehr kann ein ganzer Instrumentenkasten zum Einsatz kommen, bei dem es auch kurzfristig Änderungen bzw. Änderungsnotwendigkeiten gibt, die nicht in jedem Fall den anderen Verantwortlichen kommuniziert werden können und müssen. Aus Sicherheitsgründen und zur Wahrung von Betriebs- und Geschäftsgeheimnissen können die jeweiligen Verantwortlichen u. U. Vertraulichkeit für sich beanspruchen. Entsprechendes kann gelten, wenn einer der Verantwortlichen für seine Verarbeitung Auftragsverarbeiter in Anspruch nimmt. Die Kategorien der Auftragnehmer sind aber zumindest zu benennen (vgl. Art. 15 Abs. 1 lit. c DSGVO). Bestehen jedoch bzgl. technisch-organisatorischer Maßnahmen oder einer Auftragsverarbeitung konkret begründete Zweifel an der Rechtmäßigkeit, so besteht auch insofern ein Informationsbedarf und -anspruch der anderen Verantwortlichen.

Folgende Aspekte sind **für die Vereinbarung wesentlich**:

- verfolgte Zwecke jedes einzelnen Verantwortlichen in Bezug auf jede Datenart, also z. B. Namen, Identifizierungsdaten, IP-Adressen, Standortdaten, Kommunikationsdaten zu Zeit, Dienst, Partner, (Kommunikations-) Inhaltsdaten, evtl. differenziert nach Vertraulichkeitseinstellung der Nutzenden,
- Differenzierung nach Datenverarbeitung auf Einwilligungsbasis, auf Vertragsbasis, auf Abwägungsbasis bei (Plattform-) Mitgliedern, auf Abwägungsbasis bei Drittnutzenden,
- Differenzierung nach Sensitivität (Art. 9 DSGVO) sowie bei Kinderdatenverarbeitung (vgl. Art. 8 DSGVO),
- Übermittlung an dritte Stellen,
- insbesondere Drittlandtransfers (Art. 15 Abs. 1 lit. c DSGVO),
- Anonymisierung und Löschfristen,
- involvierte Logik beim Profiling oder bei sonstigen automatisierten Entscheidungsverfahren (Art. 15 Abs. 1 lit. h, Art. 22 DSGVO).

Hinsichtlich der Wahrnehmung der **Betroffenenrechte** können Absprachen zwischen den gemeinsam Verantwortlichen vorgenommen werden. Dazu gehört insbesondere die Information

der Betroffenen nach den Art. 13, 14 DSGVO. Bzgl. der Bearbeitung von Ansprüchen aus den Art. 15-18, 21 DSGVO können zentrale Anlaufstellen etabliert werden (Art. 26 Abs. 1 S. 3 DSGVO). Für die Umsetzung von Betroffenenrechten ist eine gegenseitige Mitteilung vorzusehen (Art. 19 DSGVO).[48]

Entgegen dem Idealbild einer gleichrangigen Vereinbarung haben bei Social Media die Plattformanbieter gegenüber den einzelnen Seiten-Betreibern und den betroffenen Nutzenden eine **einseitig bestimmende Position**. Es ist in diesen Fällen auch wegen der Massenhaftigkeit der Prozesse dann naheliegend, dass vom Plattformbetreiber vorformulierte Vereinbarungen verwendet werden. Dies ist selbst bei Auftragsverhältnissen nach Art. 28 DSGVO üblich. In diesen Fällen sind die §§ 305 ff. BGB zu den allgemeinen Geschäftsbedingungen anwendbar. In derartigen Beziehungen besteht staatlicherseits gegenüber dem schwächeren Vertragspartner eine Schutzpflicht, um zu vermeiden, dass sich die per Privatautonomie zustehende Selbstbestimmung in eine Fremdbestimmung verkehrt.[49]

Dies ist bei Social Media oft der Fall, insbesondere wenn diese eine **monopolartige Stellung** dadurch erlangen, dass ihre Nutzung durch die Nutzung der anderen potenziellen Kommunikationspartner zu einer faktischen Pflicht wird. Social Media sind für viele Menschen zur Sicherstellung ihrer Kommunikationsfähigkeit von so erheblicher Bedeutung, dass die denkbare Alternative – zur Vermeidung einer unzulässigen Datenverarbeitung, für die man verantwortlich ist – von einer Nutzung ganz abzusehen, unzumutbar ist.[50] Umgekehrt ist es den Plattformanbietern zumutbar, den anderen Verantwortlichen die von diesen benötigten Informationen zur Verfügung zu stellen. Auch die Anbieter selbst sind zur Bereitstellung dieser Informationen gegenüber den Betroffenen verpflichtet (Art. 12-15 DSGVO). Gemäß der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO obliegt es den Anbietern, diese Informationen vorzuhalten.

Eine gemeinsame Verantwortlichkeit begründet denklogisch auch jenseits der Verpflichtung zum Abschluss einer Vereinbarung **Kooperationspflichten**, soweit die gemeinsame Verarbeitung tangiert ist.[51] Dies kann immer dann relevant werden, wenn Fragen der Rechtmäßigkeit einer Verarbeitung, die von der gemeinsamen Verantwortlichkeit erfasst wird, im Raum stehen.

Kommt keine Vereinbarung zustande, weil eine Seite oder beide kein Interesse zeigen oder weil ein inhaltliches Einvernehmen nicht herstellbar ist, so kann die Aufsichtsbehörde von ihren Befugnissen nach Art. 58 DSGVO Gebrauch machen oder sie kann nach Art. 83 Abs. 4 lit. a DSGVO ein Bußgeld bis zu 10 Mio. Euro oder 2% des weltweit getätigten Umsatzes pro Geschäftsjahr verhängen.[52] Das Gleiche gilt, wenn die Vereinbarung nicht die in Art. 26 DSGVO geforderten Inhalte vorweist.[53] Entsteht durch das Fehlen einer (zureichenden) Vereinbarung ein Schaden für die Betroffenen, so haften die Verantwortlichen als **Rechtsfolge** nach Art. 82 Abs. 4 DSGVO gesamtschuldnerisch.[54] Sind von einer gemeinsamen Verantwortlichkeit mehrere Aufsichtsbehörden tangiert, so kann eine gemeinsame Kontrolle erfolgen.[55]

Ist eine gemeinsame Verantwortlichkeit tatsächlich begründet und weigert sich einer der Verantwortlichen, eine angemessene Vereinbarung zu schließen, wie kann dann ein anderer gemeinsam Verantwortlicher die Beachtung des Art. 26 DSGVO durchsetzen? Bei einer solchen **Weigerung eines Verantwortlichen** liegt wegen der gemeinsamen Festlegung von Mitteln und Zwecken einer dritte Personen betreffenden Datenverarbeitung eine vertragsähnliche faktische Beziehung vor, die ein gesetzliches Schuldverhältnis und einen Anspruch gegen die weigernde Stelle auf Abschluss der Vereinbarung nach Art. 26 DSGVO begründet. Zur Schaffung der faktischen Grundlagen für den Abschluss der Vereinbarung sowie zwecks Wahrnehmung der Pflichten als (gemeinsamer) Verantwortlicher, können von der sich weigernden Stelle die nötigen o. g. Informationen gerichtlich eingefordert werden. Zumindest eine entsprechende Klage ist in Bezug auf Facebook inzwischen anhängig.[56] Der Abschluss der Vereinbarung bzw. die Bereitstellung der dafür nötigen Informationen sind nicht vertretbare Handlungen der sich weigernden Stelle, die mit Zwangsgeld nach § 888 Abs. 1 ZPO erzwungen werden können.

Die gerichtliche Durchsetzung dieser Ansprüche erfolgt gemäß Art. 79 Abs. 2 S. 1 DSGVO vor dem Gericht des Mitgliedsstaates, in dem der sich weigernde Verantwortliche eine Niederlassung hat.[57] Diese Regelung gilt nicht nur für Betroffene i. S. v. Art. 79 Abs. 1 DSGVO, sondern generell für verantwortliche Stellen. Offenkundig ist dies, wenn, was bei Social Media regelmäßig der Fall ist, der Betroffene zugleich Verantwortlicher in Bezug auf Drittdaten ist (s. o. 3). Dies gilt aber auch in den sonstigen Fällen. Gemäß ErwGr 147 DSGVO zielt die DSGVO darauf ab, vorrangige **einheitliche Gerichtsstände** festzulegen. Für den Innenausgleich zwischen zwei Verantwortlichen sollen die Gerichte zuständig sein, die auch für die Klage eines Betroffenen wegen Rückgriff auf einen Verantwortlichen zuständig sind.[58]

5 Praxistest Facebook

Die erste Reaktion von Facebook auf die neue Rechtslage gemäß DSGVO und EuGH-Rechtsprechung war, dass beides keinerlei direkte Auswirkungen haben würde und dass „bei Bedarf“ von Facebook die nötigen Ergänzungen vorgenommen würden.[59] Als der Druck der Öffentlichkeit und von einzelnen Fanpagebetreibern größer wurde, veröffentlichte Facebook eine Ergänzung der Allgemeinen Geschäftsbedingungen (AGB) in Form eines sog. **„Controller Addendum“**, also eines „Nachtrags“.[60] Darin wird die gemeinsame Verantwortlichkeit auf die für die statistische Rückmeldung „Insights“ benötigten Daten beschränkt, die bei dem ULD-Verfahren eine Rolle spielten. Ansonsten sei Facebook „alleinig verantwortlich für die Verarbeitung solcher personenbezogenen Daten im Zusammenhang mit Seiten-Insights, die nicht unter diese Seiten-Insights-Ergänzung fallen“. Fanpagebetreiber hätten „kein Recht, die Offenlegung von im Zusammenhang mit Facebook-Produkten verarbeiteten personenbezogenen Daten von Facebook-Nutzern zu verlangen“. Die Fanpagebetreiber müssen zustimmen, „dass nur Facebook Ireland Entscheidungen hinsichtlich der Verarbeitung von Insights-Daten treffen

und umsetzen kann". Bei diesen geltend gemachte Betroffenenansprüche müssten „unverzüglich jedoch spätestens innerhalb von sieben Kalendertagen sämtliche relevanten Informationen" weitergeleitet werden.

Facebook weigert sich also ausdrücklich, mit den gemeinsam Verantwortlichen Informationen auszutauschen. Ein Mitspracherecht bzgl. der gemeinsamen Verarbeitung wird geleugnet. Die bereit zu stellenden Inhalte (s. o. 4) werden nicht zur Verfügung gestellt. Die gemeinsame Verantwortlichkeit beschränkt sich auch nicht, wie Facebook behauptet, auf die Daten, die für Insights genutzt werden. Selbst bei der restriktivsten Auslegung der EuGH-Rechtsprechung erstreckt sie sich auf die **Datenerhebung und Datenbereitstellung an Facebook** bzgl. aller Inhalts- und Nutzungsdaten von Fanpage-Nutzenden.

Die Problematik der personenbezogenen **Nutzerdaten mit Drittbezug** wird von Facebook nicht thematisiert. Vielmehr schreibt das Unternehmen in seiner „Datenrichtlinie": „Wir erfassen Informationen ... über die Personen oder Konten, mit denen du interagierst, und über die Zeit, Häufigkeit und Dauer deiner Aktivitäten".[61] Konkrete Zwecke nennt Facebook nicht: „Diese verwenden wir beispielsweise, um dir und anderen dabei zu helfen, Personen zu finden, die du möglicherweise kennst, sowie für die anderen unten aufgeführten Zwecke". Und dort heißt es: „Wir verwenden die uns zur Verfügung stehenden Informationen, um unsere Produkte bereitzustellen, also auch um Funktionen und Inhalte ... zu personalisieren und dir auf und außerhalb von Produkten Vorschläge zu unterbreiten. ... Um personalisierte Produkte zu erstellen, die individuell und für dich relevant sind, verwenden wir deine Verbindungen, Präferenzen, Interessen und Aktivitäten. Dies basiert auf den Daten, die wir von dir und anderen erfassen und erfahren (einschließlich jedweder von dir bereitgestellten Daten mit besonderem Schutz, für die du uns deine ausdrückliche Einwilligung gegeben hast); darauf, wie du unsere Produkte nutzt und mit ihnen interagierst, und auf den Personen, Orten oder Dingen, mit denen du auf und außerhalb von unseren Produkten verbunden bzw. an denen du interessiert bist."

Letztlich werden für die Verarbeitung von Daten **keinerlei Einschränkungen** gemacht bzgl. Art der Daten, Art der Auswertung, Art der Nutzung und Zwecke, Art der Empfänger. Von einer wirksamen Einwilligung zur Verarbeitung sensitiver Daten kann keine Rede sein. Dass eine gemeinsame Verantwortlichkeit mit den Nutzenden bestehen könnte, ist nicht im Ansatz erkennbar.

6 Schlussbemerkung

Über die Konsequenzen gemeinsamer Verantwortlichkeit bei Social Media hat die **Diskussion eben erst begonnen**. Dies ist erstaunlich angesichts des Umstands, dass der vom EuGH festgestellte rechtliche Rahmen spätestens seit 1995, also dem Inkrafttreten der europäischen Datenschutzrichtlinie besteht. Die Datenschutzaufsichtsbehörden haben das Thema seit gut zehn Jahren benannt, doch konnten sie bis heute die erkannten rechtlichen Schlussfolgerungen gegenüber den Social-Media-Anbietern nicht durchsetzen. Ob sich das künftig angesichts der katastrophalen personellen Ausstattung der Datenschutzaufsicht und des fehlenden politischen Rückhalts durch Regierungen und Öffentlichkeit mit der DSGVO ändern wird, muss leider bezweifelt werden.

Der zu ziehende Schluss ist, dass die Verantwortungslosigkeit im Internet vorläufig fortgeschrieben wird. Dies darf nicht einmal auf kurze Sicht hingenommen werden. Social Media im Internet sind eine grundrechtsintensive Sphäre. Durch eine weitere Verlagerung von immer mehr Aktivitäten ins Internet und insbesondere auf Social Media mit einer hohen Arbeitsteilung nehmen die Verantwortlichkeiten für **grundrechtsrelevante Vorgänge** zu. Werden die Verantwortlichen nicht zur Verantwortung gezogen, so bedeutet dies Fortführung der Anarchie – nicht im Sinne einer herrschaftslosen digitalen Gesellschaft, sondern im Sinne der Herrschaft der digital und ökonomisch Mächtigen.

Verantwortungslosigkeit ist nicht zwangsläufig. Möglich ist auch, dass die datenschutzrechtliche Regulierung wirksam umgesetzt wird. Hierfür haben wir unabhängige Aufsichtsbehörden und unabhängige Gerichte. Diese können künftig schmerzhafte Bußgelder aussprechen. Letztlich wird es aber künftig nicht ohne klare Verbote und Untersagungen gehen. Damit die Behörden und Gerichte unabhängige und wirksame Entscheidungen treffen und auch deren Vollzug durchsetzen, benötigen sie die dafür nötigen Ressourcen und zugleich den nötige ideellen Rückhalt. Dafür bedarf es auch einer verstärkten Fortführung der Debatte über digitale Verantwortung – ethisch, rechtlich und technisch-organisatorisch.

1 Weichert DuD 2012, 716 ff.

2 Dagegen Weichert DANA 1/2012, 19.

3 Eine umfassende Dokumentation aller Vorgänge in dem ULD-Verfahren findet sich unter https://www.datenschutzzentrum.de/plugin/tag/facebook.

4 VG Schleswig 09.10.2013 – 8 A 14/12, ZD 2014, 51; K&R 2013, 824, DuD 2014, 120; DANA 2014, 169; dazu Karg ZD 2014, 54 ff., Weichert ZD 2014, 1 f.

5 OVG Schleswig-Holstein 04.09.2014– 4 LB 20/13, DuD 2014, 869, ZD 2014, 643; K&R 2014, 831; CR 2014, 801; DANA 2014, 184.

6 ULD: „OVG-Urteil zu Facebook-Fanpages revisionsbedürftig", 19.09.2014, https://www.datenschutzzentrum.de/artikel/770-ULD-OVG-Urteil-zu-Facebook-Fanpages-revisionsbeduerftig.html#extended.

7 Z. B. Petri ZD 2015, 103; Martini/Fritzsche, NVwZ-extra 21/2015; schon früh Spindler, Gutachten zum 69. Deutschen Juristentag, 2012, F 81 f.

8 BVerwG 25.02.2016 – 1 C 28.14, DuD 2016, 537; CR 2016, 729; NVwZ 2016, 1737; K&R 2016, 437.

9 http://curia.europa.eu/juris/document/document.jsf?text=&docid=195902&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1.

10 EuGH 05.06.2018 – C-210/16, NJW 2018, 2537; NVwZ 2018, 1386; GRUR Int. 2018, 853; EuZW 2018, 534; NZA 2018, 919; MMR 2018, 591; MIR 2018, Dok. 026; BB 2018, 1480; dazu mit Hinweisen auf die Reaktionen Weichert DANA 2018, 98 ff.; vgl. von dem Bussche BB 2018, 1782; Härting/Gössling NJW 2018, 2523.

11 EuGH 05.06.2018 – C-210/16 Rn. 27 mit Verweis auf Art. 2 lit. d EG-DSRl; ebenso Art. 4 Nr. 7 DSGVO.

12 EuGH 05.06.2018 – C-210/16 Rn. 28.

13 EuGH 05.06.2018 – C-210/16 Rn. 32.

14 EuGH 05.06.2018 – C-210/16 Rn. 36.

15 EuGH 05.06.2018 – C-210/16 Rn. 38, ebenso später EuGH 10.07.2018 – C-25/17 Rn. 68, NVwZ 2018, 1787; EuZW 2018, 897; NZA 2018, 991; DANA 2018, 156.

16 EuGH 05.06.2018 – C-210/16 Rn. 39.

17 EuGH 05.06.2018 – C-210/16 Rn. 40.

18 EuGH 05.06.2018 – C-210/16 Rn. 41.

19 EuGH 05.06.2018 – C-210/16 Rn. 43.

20 EuGH 10.07.2018 – C-25/17 Rn. 66.

21 EuGH 10.07.2018 – C-25/17 Rn. 70-73.

22 EuGH 10.07.2018 – C-25/17 Rn. 68; ebenso z. B. Martini in Paal/Pauly Art. 26 Rn. 18, 20.

23 EuGH 10.07.2018 – C-25/17 Rn. 68.

24 OLG Düsseldorf 19.01.2017 – I-20 U 40/16, GRUR 2017, 416; GRUR Int. 2017, 466; K&R 2017, 196; Vorinstanz LG Düsseldorf 09.03.2016 – 12 O 151/15, NJ 2016, 257; MMR 2016, 328; K&R 2016, 364; CR 2016, 372.

25 Generalanwalt Bobek, Gerichtshof der Europäischen Union Pressemitteilung Nr. 206/18 v. 19.12.2018, https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-12/cp180206de.pdf.

26 Ingold in Sydow, Europäische Datenschutzgrundverordnung, 2017, Art. 26 Rn. 4; Hartung in Kühling/Buchner, DS-GVO – BDSG, 2. Aufl. 2018, Art. 26 Rn. 12; Martini in Paal/Pauly, Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2. Aufl. 2017, Art. 26 Rn. 3.

27 Bertermann in Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 26 Rn. 8; Hartung in Kühling/Buchner (Fn. 26) Art. 26 Rn. 16.

28 Schantz in Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 371.

29 BGH 12.07.2018 – III ZR 183/17 Rn. 44; NJW 2018, 3178; MDR 2018, 1002; MMR 2018, 740; K&R 2018, 633.

30 Weichert in Däubler/Wedde/Weichert/Sommer, EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, § 13 TMG Rn. 36.

31 Schantz in Schantz/Wolff (Fn. 28) Rn. 372; Dovas ZD 2017, 514; Däubler in Däubler u. a. (Fn. 30) Art. 26 Rn. 8; Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 2016, § 1 Rn. 60; Piltz in Gola, DS-GVO, 2017, Art. 26 Rn. 8; Ingold in Sydow (Fn. 26) Art. 26 Rn. 5; Bertermann in Ehmann/Selmayr (Fn. 27) Art. 26 Rn. 12; Hartung in Kühling/Buchner (Fn. 26) Art. 26 Rn. 20.

32 Laue/Nink/Kremer (Fn. 31) § 1 Rn. 55.

33 A. A. Schantz in Schantz/Wolff (Fn. 28) Rn. 371

34 Hartung in Kühling/Buchner (Fn. 26) Art. 26 Rn. 20; Martini in Paal/Pauly (Fn. 26) Art. 26 Rn. 3.

35 Ingold in Sydow (Fn. 26) Art. 26 Rn. 7; a. A. Piltz in Gola (Fn. 31) Art. 26 Rn. 17.

36 Martini in Paal/Pauly (Fn. 26) Art. 26 Rn. 9.

37 Martini in Paal/Pauly (Fn. 26) Art. 26 Rn. 10.

38 So ausdrücklich Ingold in Sydow (Fn. 26) Art. 26 Rn. 9; ebenso Martini in Paal/Pauly (Fn. 26) Art. 26 Rn. 10.

39 Piltz in Gola (Fn. 31) Art. 26 Rn. 9 f.; Hartung in Kühling/Buchner (Fn. 26) Art. 26 Rn. 9.

40 Däubler in Däubler u. a. (Fn. 30) Art. 26 Rn. 11; Laue/Nink/Kremer (Fn. 31) § 1 Rn. 63.

41 So ausdrücklich Bertermann in Ehmann/Selmayr (Fn. 27) Art. 26 Rn. 12.

42 Schantz in Schantz/Wolff (Fn. 28) Rn. 372; Martini in Paal/Pauly (Fn. 26) Art. 26 Rn. 25.

43 Martini in Paal/Pauly (Fn. 26) Art. 26 Rn. 23.

44 Martini in Paal/Pauly Art. 26 (Fn. 26) Rn. 23a.

45 Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) 06.06.2018, Die Zeit der Verantwortungslosigkeit ist vorbei; https://www.datenschutzzentrum.de/uploads/facebook/2018-06-05-Entschliessung-DSK-Fanpages-EuGH-Urteil.pdf.

46 DSK 06.06.2018 (Fn. 45), DSK, 05.09.2018, Beschluss zu Facebook-Fanpages, https://datenschutz-hamburg.de/assets/pdf/DSK-Beschluss_zu_Facebook_Fanpages.pdf; zum Dienst Facebook Custom Audience, VGH München 26.09.2018 – 5 CS 18.1157, K&R 2018, 810; VG Bayreuth 08.05.2018 – B 1 S 18.105, K&R 2018, 524; DANA 2018, 222.

47 DSK 05.09.2018 (Fn. 46), die letzten beiden Absätze.

48 Vgl. Hartung in Kühling/Buchner (Fn. 26) Art. 26 Rn. 25.

49 BVerfG 23.10.2006 – 1 BvR 2027/02 Rn. 35, MMR 2007, 93, DuD 2006, 817; VersR 2006, 1669; WM 2006, 2270; DVBl 2007, 111.

50 BVerfG 23.10.2006 – 1 BvR 2027/02 Rn. 36.

51 Laue/Nink/Kremer (Fn. 31) § 1 Rn. 61.

52 Däubler in Däubler u. a. (Fn. 31) Art. 26 Rn. 8; Schantz in Schantz/Wolff (Fn. 28) Rn. 373.

53 Ingold in Sydow (Fn. 26) Art. 26 Rn. 9; Martini in Paal/Pauly (Fn. 26) Art. 26 Rn. 22.

54 Däubler in Däubler u. a. (Fn. 30) Art. 26 Rn. 14; Plath in Plath, BDSG DSG-VO, 2. Aufl. 2016, Art. 26 Rn. 9; Schantz in Schantz/Wolff (Fn. 28) Rn. 377; Laue/Nink/Kremer (Fn. 31) § 1 Rn. 54; Hartung in Kühling/Buchner (Fn. 26) Art. 26 Rn. 29.

55 Piltz in Gola (Fn. 31) Art. 26 Rn. 7.

56 BT-Fraktion Bündnis 90/Die Grünen, PM 02.10.2018, Klage gegen Facebook, https://www.gruene-bundestag.de/netzpolitik/klage-gegen-facebook.html.

57 Bergt in Kühling/Buchner (Fn. 26) Art. 79 Rn. 16.

58 Vgl. EuGH 15.06.2017 – C-249/16 Rn. 31; NJW 2018, 845; ZIP 2017, 1734.

59 Dokumentiert in Weichert DANA 2018, 100.

60 Seiten-Insights-Ergänzung bezüglich des Verantwortlichen, https://www.facebook.com/legal/terms/page_controller_addendum.

61 Datenrichtlinie, https://de-de.facebook.com/policy.php.

Klaus-Jürgen Roth

Der Prominentenhack und Lehren daraus

Social Media – sog. soziale Medien – lassen die Grenzen zwischen Privatem und Öffentlichem verschwinden – in vieler Hinsicht. Das Private eignet sich die Öffentlichkeit an. Es gilt aber auch die umgekehrte Aussage: Die Öffentlichkeit eignet sich das Private an – und wird dadurch schnell asozial. Für diese These gibt es schon abermillionen Beispiele. Ein Anschauliches war nun der Anfang 2019 bekannt gewordene Prominentenhack.

Das Jahr 2019 begann für 993 Prominente in Deutschland unerfreulich: Am 03.01. wurde über Radio Berlin Brandenburg (RBB) öffentlich bekannt, dass im Laufe des Dezembers persönliche Daten und parteiinterne Dokumente Hunderter deutscher PolitikerInnen und anderer Personen des öffentlichen Lebens in einem „Adventskalender" über den Twitter-Account @_0rbit veröffentlicht worden sind. Der RBB war auf den Vorgang aufmerksam geworden, als der Youtube-Star Simon Unge seinen mehr als 2 Mio. Followern mitgeteilt hatte, gehackt worden zu sein. Hinter den virtuellen Türchen des Accounts führten Links zu den Informationen, die auf dem Blogspot-Account von 0rbiter und bei diversen Filehostern zu finden waren. Zwar wurden keine politisch brisanten Dokumente veröffentlicht, sehr wohl aber viele persönliche Dokumente wie Briefe, Rechnungen und Einzugsermächtigungen. In den Archiven fanden sich teilweise Chats mit Familienmitgliedern und Kreditkarteninformationen.

- Betroffene

Betroffen waren die Bundeskanzlerin Angela Merkel und der Bundespräsident Frank-Walter Steinmeier, Abgeordnete aus dem Bundestag, die Parteichefs Christian Lindner, Andrea Nahles und Robert Habeck, die Bundesminister Jens Spahn und Heiko Maas, Abgeordnete aus den Landtagen, aus dem Europaparlament und aus kommunalen Einrichtungen. Besonders abgesehen hatte es der Hacker auf die Grünen, u. a. den Bundestagsabgeordneten Konstantin von Notz und besonders stark Parteichef Habeck, dieser mit Bankdaten, Mailadresse, Familienfotos und Chats mit seiner Frau und seinen Söhnen. Von Eva von Angern, Landtagsabgeordnete der Linken in Sachsen-Anhalt, waren rund 200 private Dokumente ins Netz gestellt. Der Spiegel machte eine zahlenmäßige Aufstellung nach Parteizugehörigkeit: CDU/CSU 425, SPD 318, Die Linke 112, Grüne 110, FDP 28.

Betroffen waren aber auch JournalistInnen, z. B. von ARD und ZDF, und Künstler, etwa Til Schweiger, Youtuber wie Gronkh, Rapper wie Sido, Marteria und K.I.Z., Komiker wie Nico Semsrott und Christian Ehring oder politische Aktivisten wie Jürgen Resch, Geschäftsführer der sich für Dieselfahrverbote engagierenden Deutschen Umwelthilfe (DUH). Verschont geblieben sind rechte PolitikerInnen, etwa von der AfD. Von Jan Böhmermann wurden besonders umfangreiche Unterlagen veröffentlicht: Adressen, Bankdaten, Rechnungen, Fotos und Namen seiner Kinder. Böhmermann war schon zuvor Opfer von digitalen Übergriffen, nachdem er am 26.04.2018 in der ZDF-Sendung „Neo Magazin Royale" und auch auf YouTube ein Video veröffentlichte, das die rechte Netzaktion „Reconquista Germanica" angreift und zur digitalen Gegenbewegung „Reconquista Internet" aufrief. Der „Adventskalender" von 0rbit enthielt mehr als 2.000 Links zu Dokumenten, allein zu Personen aus dem Politikbereich fanden sich rund 8.000 E-Mail-Nachrichten, 35.000 Bilder, 600 Videos, 4.000 PDF- und 1.600 Word-Dokumente.

- Coming out

Bundesinnenminister Horst Seehofer (CSU) erklärte nach Bekanntwerden der Leaks umgehend: „Es wird mit Hochdruck daran gearbeitet, den Urheber der Veröffentlichung ausfindig zu machen und den Zugriff auf die Daten schnellstmöglich zu unterbinden". Tatsächlich forderte der für Twitter in Deutschland zuständige Datenschutzbeauftragte Johannes Caspar schon am nächsten Tag nach dem Bekanntwerden Twitter auf, die auf die privaten Infos von Politikern verweisenden, in einer Liste aufgeführten Links umgehend zu deaktivieren. Dies erfolgte in Bezug auf „0rbit", zunächst aber nicht bzgl. der Retweets und Likes anderer Nutzender. Das Twitter-Konto @_0rbit hatte fast 19.000 Follower. Der Account @_0rbit gehörte in der Vergangenheit dem YouTuber Yannick Kromer, auch bekannt als Dezztroyz, der gut 190.000 AbonnentInnen damit bespaßt hatte, dass er Minecraft-Spielende trollte und Videos von den Aktionen veröffentlichte. Mai 2016 scheint Dezztroyz die Kontrolle über das seit Anfang 2015 bestehende Twitter-Konto verloren zu haben.

Auslöser der strafrechtlichen Ermittlungen war wohl, dass ein Mitarbeiter des ehemaligen SPD-Kanzlerkandidaten Martin Schulz der Polizei Aachen mitteilte, Schulz sei mehrfach von Fremden auf seiner vertraulichen Handynummer angerufen worden. Kurze Zeit später erhielt das Büro der SPD-Fraktionschefin Andrea Nahles den Hinweis, dass von ihr private Daten im Internet zu finden seien. Eine Nachfrage des Büros ergab, dass Nahles bereits anonyme Anrufe erhalten hatte. Daraufhin bat am 03.01.2019 um 22:40 ein führender Mitarbeiter von Nahles per Mail das Lagezentrum des Bundeskriminalamtes (BKA) in Wiesbaden um Aufklärung.

- Ermittlungen

In die Täterermittlung waren dann auch das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundesamt für Verfassungsschutz (BfV) und die Bundespolizei einbezogen. Die Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) bei der Generalstaatsanwaltschaft Frankfurt am Main

übernahm die Leitung der Ermittlungen. Der Generalbundesanwalt leitete ein „Beobachtungsverfahren“ ein. Dessen Bundesanwaltschaft ist gefordert, wenn eine geheimdienstliche Agententätigkeit zu vermuten ist. Auch der Bundesnachrichtendienst (BND) soll als Auslandsgeheimdienst in die laufenden Untersuchungen involviert worden sein, da zunächst nicht ausgeschlossen wurde, dass z. B. russische Hacker hinter dem Angriff stehen. Die zentrale Koordination der Ermittlungen übernahm das nationale Cyber-Abwehrzentrum.

Dem BSI waren Vorgänge aus dem Hack bereits seit Wochen bekannt. Sein Präsident, Arne Schönbohm, erklärte, dass man schon sehr frühzeitig im Dezember mit einzelnen betroffenen Abgeordneten dementsprechend gesprochen hätte. In den vergangenen Monaten hatten sich sieben Bundestagsabgeordnete beim BSI mit vergleichbaren Vorgängen gemeldet. Es seien Gegenmaßnahmen eingeleitet worden. Unter anderem sei ein Spezialteam für Hilfestellungen bei Betroffenen (Mobile Incident Response Team) losgeschickt worden: „Von daher gab es schon frühzeitig bestimmte Aktionen.“ Burkhard Lischka, der innenpolitische Sprecher der SPD-Bundestagsfraktion zeigte sich beunruhigt über das Eingeständnis des BSI: „Sollte sich herausstellen, dass das BSI schon vor Wochen von Veröffentlichungen gehackter Daten wusste, ohne die anderen Sicherheitsbehörden zu informieren, ist dies vollkommen inakzeptabel und wirft kein gutes Licht auf die Zusammenarbeit unserer Sicherheitsbehörden im Bereich der Cybersicherheit.“ Das BKA erklärte, erst zeitgleich mit den Medienberichten von dem Vorgang erfahren zu haben.

Schnell ergab sich, dass die geklauten Daten aus verschiedenen Hacks von Konten der Betroffenen etwa auf der Amazon-Cloud, Facebook oder Twitter stammen und mit viel Fleißarbeit zusammengetragen wurden. Zumeist veröffentlichte 0rbit Telefonnummern und private Anschriften. Von 14 Personen war es sehr viel mehr, darunter Chats, Bankkontodaten, Ausweiskopien, E-Mails und private Fotos. Bei 44 Nutzenden hatte er offenbar Zugriff auf das Facebook-Konto. Zum Teil nutzte 0rbit offenbar Sicherheitslücken, die die Betroffenen selbst mit verursacht hatten. Teilweise gelangte er an Daten über Angehörige oder Freunde. Die Kopie aus dem Familienchat von Robert Habeck stammte offenbar aus dem Facebook-Account seiner Frau, deren E-Mail-Adresse wiederum knapp ein Jahr zuvor in einer Liste vom 80 Mio. Log-in-Daten auftauchte, die Unbekannte ins Netz gestellt hatten.

- Ermittlungserfolg

Die entscheidenden Hinweise auf den Promi-Hacker 0rbit lieferte dann offenbar der 19-jährige IT-Experte Jan Schürlein. Die Wohnung Schürleins war von Strafverfolgern durchsucht worden, nachdem er öffentlich zu Protokoll gegeben hatte, dass er wisse, wer der Urheber des Datenskandals sei. Schürlein hatte das BKA auch auf die Fährte eines anderen Ermittlungsverfahrens gegen 0rbit aus dem Jahr 2016 gebracht. Damals war 0rbit demnach unter dem Pseudonym Nullr0uter unterwegs. Er nannte sich an anderer Stelle auch „God“. Weiter werden ihm die Spitznamen dennis 567 und r00taccess zugeschrieben. Durch das alte Ermittlungsverfahren sollte es den Beamten leicht gefallen sein, 0rbit aufzuspüren. Denn 2016 hatte er seine IP-Adresse und damit den Internetanschluss seiner Eltern verraten.

Schürlein hatte den Täter über Twitter kennengelernt. Als Teil der Security-Szene rund um YouTube und Gamer-Chatnetzwerke wie Discord seien ihm dessen Doxing-Aktionen und die Account-Übernahme von 0rbit schon vor Jahren aufgefallen. Er habe über die Jahre immer wieder Kontakt mit dem Hacker gehabt. Er habe seine Informationen über 0rbit den Strafverfolgern nur preisgegeben, weil er keine andere Wahl gehabt habe. Ein Bekannter habe das BKA darauf hingewiesen, dass er mit dem Hacker in Kontakt stehe.

Am Sonntagmittag, dem 06.01.2018, war gemäß BKA-Angaben der mutmaßliche Täter des Hackings identifiziert. In den Medien wird er Johannes S. genannt. Es handelt sich um einen 20jährigen Mann aus Homberg (Ohm) in Mittelhessen, einen Computerfan und Technikfreak, der sich sozusagen im Selbststudium neben der Schule zu einem Hacker entwickelte und von seinem Kinderzimmer aus seine Aktionen durchführte. Angesichts der öffentlichen Aufregung, die er mit seinem Doxing verursachte, hatte er es schon mit der Angst zu tun bekommen und versucht, zumindest einen seiner inkriminierenden Datenträger zu vernichten. Die Polizei hat diesen sichergestellt und versucht, die Daten wieder herzustellen. Die Fahnder äußerten den Eindruck, dass dem jungen, geständigen Mann die Reichweite seines Tuns lange Zeit nicht bewusst war. Erst als die Polizei auftauchte, ihn kurzzeitig festnahm und die elterliche Wohnung durchsuchte, sei ihm klargeworden, was er getan hat. Eine Flucht- oder Verdunkelungsgefahr sahen die Ermittler nicht. Als Motiv soll der junge Mann angegeben haben, er habe sich über Äußerungen von Politikern geärgert.

Innenminister Seehofer präsentierte – eingerahmt von BKA-Chef Holger Münch und BSI-Chef Arne Schönbohm – stolz das schnelle Ermittlungsergebnis. Die Bundesregierung prüfe nun unter anderem die Schaffung eines Frühwarnsystems in Verbindung mit einer rund um die Uhr einsetzbaren Crew im BSI. Der Gesetzentwurf für ein zweites IT-Sicherheitsgesetz soll bald fertig werden. Ein Eckpunktepapier aus Oktober 2018 sieht vor, das BSI im Verbraucherschutz zu stärken und seine Möglichkeiten zum Schutz von Wahlen auszuweiten. Providern sollen zusätzliche Informationspflichten gegenüber ihren KundInnen auferlegt werden. Das BSI soll in besonderen Gefahrenlagen ein Weisungsrecht gegenüber Wirtschaftsunternehmen erhalten. Zudem wolle man die Menschen verstärkt über Gefahren im Netz aufklären. Deutlich mehr Stellen bei BKA und BSI seien bereits vom Bundestag bewilligt.

- Der Täter

Für die Staatsanwaltschaft Gießen war Johannes S. kein Unbekannter. Sie hatte in den vergangenen Jahren drei Ermittlungsverfahren gegen ihn eingeleitet, u. a. wegen des Verdachts des Ausspähens von Daten und der Fälschung beweiserheblicher Daten. Alle drei Verfahren sind noch nicht abgeschlossen. Die Akten hat nun die Generalstaatsanwaltschaft Frankfurt am Main übernommen.

Die Ermittler unterstellen 0rbit keine politische Motivation. In der Youtube-Szene ist er schon lange präsent. Der 28jährige Youtuber Thomas Hackner hatte mit 0rbit seit 2015 Kontakt und schildert ihn zunächst als „sehr zurückhaltend und vor allem sehr jung. Er wollte mit seinen Erfolgen prahlen“. Der 18jährige Levi Pennel will ihn ebenfalls kennengelernt haben und beschreibt ihn wie folgt: „Zuletzt hat er sich politisch in eine immer rechtsradikalere Richtung entwickelt und sich immer stärker politisiert. Während anfangs noch lediglich kleinere Ziele das Opfer waren und das Motiv meist Aufmerksamkeit, mischte sich mit der Zeit immer mehr eine politische Komponente dazu.“ Johannes S. soll vor allem von „Die vulgäre Analyse“ beeinflusst worden sein, einem Kanal eines YouTubers, der mit Islamhass besonders auffällt und der sich in seinen Videos bereits mit einigen der Opfern des jüngsten Datenklaus befasst hatte. In den Kommentarspalten des Kanals mischten Führungspersonen der rechtsextremen „Identitären Bewegung“ mit.

Ein Hinweis des Verfassungsschutzes soll bei der schnellen Identifizierung geholfen haben. S. erwies sich als ein ziemlicher Schwätzer; Spuren von ihm fanden sich in zahlreichen Foren. Gegenüber der Justiz behauptet der 20-Jährige noch immer, allein gehandelt zu haben. Als BKA-Beamte ihm aber einen Computer zuschoben und aufforderten, doch einmal zu zeigen, wie er das gemacht habe, scheiterte S. Die Ermittlungen gehen weiter.

Reaktionen

- Politik

Der stellvertretende Vorsitzende der SPD-Fraktion, Carsten Schneider, betonte, der demokratische Wettbewerb lasse sich nicht „durch auf illegale Weise gewonnene persönliche Daten kompromittieren“: „Die IT-Infrastruktur der SPD-Bundestagsfraktion selbst ist nicht betroffen.“ Man habe Sicherheitsmaßnahmen eingeleitet, „um den Schutz der Kommunikation und die Funktionsfähigkeit der parlamentarischen Arbeit zu gewährleisten“. Bundesjustizministerin Katarina Barley verurteilte umgehend das Vorgehen des noch unbekannten Cyberkriminellen auf Twitter als einen „schwerwiegenden Angriff auf das Recht auf Privatsphäre und damit einen Grundpfeiler unserer Demokratie“. Die Urheber wollten Vertrauen in den liberalen Rechtsstaat und seine Institutionen beschädigen: „Kriminelle und ihre Hintermänner dürfen keine Debatten in unserem Land bestimmen.“

Jan Philipp Albrecht, ehemaliger EU-Parlamentarier und nun für Digitales zuständiger Minister in Schleswig-Holstein erklärte: „Für die Betroffenen ist das aktuelle Leak ein tiefer Eingriff und teilweise eine Gefährdung bis ins familiäre Umfeld“. Der Vorfall zeige, wie groß die Sicherheitslücken bei IT-Kommunikationsdiensten noch immer seien: „Hier haben Bundesregierung und EU-Kommission viel zu lange gepennt und dem Druck der Internetanbieter nachgegeben“.

Jan Korte, Geschäftsführer der Linksfraktion, erklärte: „Wer private Angaben von Personen veröffentlicht, nimmt deren Gefährdung billigend in Kauf, und dagegen müssen wir uns gemeinsam wehren“. Die linke Digitalexpertin Anke Domscheit-Berg ergänzte, der Hack sei „eine Folge der vernetzten Gesellschaft“. Das schwächste Glied in einer Kette müsse dabei gar nicht „der Promi oder Politiker selbst sein“. In Frage kämen auch Dritte, auf deren Adressbuch im Smartphone oder Plattformen bis hin zum Sexshop jemand Zugriff erlangt hat. Der linke Abgeordnete Diether Dehm warnte davor, vorschnell Russland zu verdächtigen. Sollte „von den üblichen Medienagenten“ Wladimir Putin für den Hackerangriff verantwortlich gemacht werden, werde er seinen zunächst gestellten Strafantrag gegen Unbekannt zurückziehen.

Der Vorsitzende des Bundestagsausschusses Digitale Agenda, Jimmy Schulz (FDP), prognostizierte: „Diese Art der Hackerangriffe und Datenleaks sind leider kein Novum mehr und wird es in Zukunft öfter geben. Gerade weil es eine der zentralen staatlichen Aufgaben ist, die Privatsphäre der Menschen zu schützen, müssen wir dies zum Anlass nehmen, uns fraktionsübergreifend für die IT-Sicherheit Deutschlands einzusetzen.“ Die Liberalen hätten bereits einen Antrag zum „Recht auf Verschlüsselung“ ins Parlament eingebracht. Darüber hinaus dürfte der Staat selbst „nicht an der Schwächung der IT-Sicherheit arbeiten“.

Patrick Breyer, Spitzenkandidat der Piratenpartei zur Europawahl, meinte, dass es unverantwortlich sei, dass selbst prominente Bundespolitiker ihre Gesprächspartner großen US-amerikanischen Digitalkonzernen auslieferten. Der Bundestag müsse jetzt dringend einen „Verhaltenskodex zum Schutz der Sicherheit mandatsbedingter Kontakte“ ausarbeiten.

Die von den Hacks nicht betroffene AfD äußerte sich – soweit erkennbar – offiziell nicht zu den Hacks.

- IT-Sicherheit

Norbert Pohlmann, Vorstand für IT-Sicherheit beim eco-Verband der Internetwirtschaft, appellierte an die Bundesregierung, „die Entwicklung und Verbreitung einfach anwendbarer Verschlüsselungstechnologien stärker zu fördern und voranzutreiben“. Von Maßnahmen wie Backdoors, Zero Day Exploits und Staatstrojaner müssten die Politik und die Behörden dagegen „entschieden Abstand nehmen“, da sie den Aufbau sicherer IT-Systeme unterwanderten. Für Michael Littger von der Initiative „Deutschland sicher im Netz“ zeigte die Attacke „den Nachholbedarf beim Thema digitale Aufklärung“ auf. Es müsse darum gehen, „digitale Kompetenzen in allen Lebensbereichen zu verankern“. Einfache Schutzfähigkeiten reichten, „um rund 90 Prozent der Cyberangriffe abzuwehren“.

BSI-Chef Schönbohm machte deutlich, dass bei der Abwehr solcher Angriffe noch einiges zu tun sei: „Es ist ein kontinuierlicher Prozess. Und da werden wir alle gemeinsam – Staat, Wirtschaft und Gesellschaft – noch besser werden müssen, um es den Angreifern schwieriger zu machen.“ Es gelte aber der Illusion einer völligen Sicherheit vorzubeugen: „Das ist ein normales Einhergehen mit der Digitalisierung, dass wir immer wieder auch erfolgreiche Angriffe haben. Wir haben auch jeden Tag eine Vielzahl von Wohnungseinbrüchen.“

Politische Forderungen

Die Grünen im Bundestag beantragten umgehend eine Sondersitzung der

Kommission für den Einsatz neuer Informations- und Kommunikationstechniken sowie des Innenausschusses des Bundestags. Fraktionsvize Konstantin von Notz erklärte: „Wir brauchen endlich echte proaktive Maßnahmen zur Erhöhung der IT-Sicherheit. Dazu gehören unter anderem ein Verzicht auf den staatlichen Handel mit Sicherheitslücken, durchgehende Ende-zu-Ende-Verschlüsselungen und die Stärkung unabhängiger Aufsichtsstrukturen."

Die SPD-Netzpolitikerin Saskia Esken forderte einen bewussteren Umgang mit Passwörtern und mehr Verschlüsselung. Das Bundesinnenministerium müsse eine „Plakatkampagne zur IT-Sicherheit" durchführen. Die Gesellschaft müsse lernen, besser mit Desinformationsstrategien im Netz umzugehen, um „resilient zu bleiben". Die von der Regierung erörterten „Hackbacks" brächten dagegen nichts.

Der Cyber-Sicherheitsrat Deutschland mahnte als Konsequenz aus dem Hackerangriff einen Ausbau der Cyber-Abwehrkapazitäten an. Ziel müsse sein, Angriffe schneller zu entdecken sowie Cyberkriminelle effektiv zu identifizieren und strafrechtlich verfolgen zu können. Gemäß dem Präsidenten Wilhelm Dünn zeigt der Vorfall, wie akut und ernst die Gefahren aus dem Cyberraum sind. Nicht nur für die Wirtschaft, sondern auch gegenüber politischen Systemen – insbesondere Demokratien – und der Gesellschaft könne die voranschreitende, weltweite Vernetzung für solche Kampagnen missbraucht werden und großen Schaden anrichten. Betreiber von Instant-Messaging- und Mikroblogging-Plattformen sowie sozialen Netzen müssten sich stärker für die Unterbindung derartiger schmutziger Aktionen einsetzen. Das seit dem 01.01.2018 in Kraft befindliche Netzwerkdurchsetzungsgesetz müsse entsprechend überarbeitet und erweitert werden. Eine Art Frühwarnmechanismus sei wünschenswert.

Bundesjustizministerin Katarina Barley (SPD) brachte die eben per Gesetz eingeführte Verbraucher-Musterklage gegen Twitter und Facebook ins Gespräch: „Sollten im Zusammenhang mit dem Datenleak Haftungsansprüche gegen Unternehmen bestehen, könnten betroffene Verbraucher sie gemeinsam im Rahmen einer Musterfeststellungsklage geltend machen." Durch eine solche Klage könnte überprüft werden, ob ein Internetkonzern alles in seiner Macht Stehende getan hat, um Schäden abzuwenden.

Der Chef der CDU-Bundestagsfraktion Ralph Brinkhaus plädierte für härtere Strafen. Bislang könne das sogenannte Ausspähen von Daten mit Freiheitsstrafe von maximal drei Jahren geahndet werden: „Wir sollten prüfen, das Strafmaß bei schweren Cyberdelikten anzuheben." Thomas Tschersich, seit 2014 Leiter Cybersicherheit bei der Deutschen Telekom, kritisierte: „Viele Gerichte behandeln den digitalen Einbruch immer noch wie ein Kavaliersdelikt". Viele Menschen speicherten auf ihren Computern Informationen, die wertvoller seien als die Gegenstände in ihrer Wohnung: „Also sollte der digitale Einbruch genauso hart bestraft werden wie der tatsächliche Wohnungseinbruch." Leider fehle bei vielen Richtern das nötige IT-Wissen; hier seien dringend Nachschulungen und ein gemeinsamer Wissensaustausch nötig. Der Grüne Konstantin von Notz erklärte unter Hinweis darauf, dass Hackerangriffe auf Abgeordnete, JournalistInnen und Personen des öffentlichen Lebens ein Angriff auf die Demokratie seien: „Es lohnt sich deshalb, darüber nachzudenken, ob es sinnvoll wäre, auf solche Angriffe mit besonderer Strenge zu reagieren." SPD-Innenpolitiker Burkhard Lischka meinte dagegen, statt schärferer Gesetze halte er es für sinnvoller, die zersplitterten Zuständigkeiten bei der Abwehr von Cyberkriminalität zu einen.

- Offizielle erste Reaktionen

Die Cyber-Abwehr in Deutschland soll schon länger reformiert werden. Als die Aufregung um den Hackerangriff auf deutsche Prominente auf ihrem Höhepunkt war, meldete sich der parlamentarische Staatssekretär im Bundesinnenministerium Stephan Mayer zu Wort. Man sei entschlossen, das Cyber-Abwehrzentrum in Bonn schnell zu reformieren, auszubauen, schlagkräftiger zu machen. Der Auftrag für eine solche Reform, für ein „Cyber-Abwehrzentrum plus", stammt bereits aus dem Jahr 2015. Außer einer Reihe von Sitzungen und dem Austausch von immer neuen Konzepten war bisher nicht viel geschehen. Die dort sitzenden neun Behörden – darunter das BKA, das BSI und das BfV – taten sich schwer, sich zu einigen. Die digitale Wacht am Rhein funktioniert bisher nicht gut genug. Es gibt nicht einmal einen Dienst rund um die Uhr.

Nun soll es schnell gehen. Das Innenministerium macht Druck, Spitzentreffen sind anberaumt. Um die zersplitterten Zuständigkeiten in der Cyber-Abwehr zu bündeln, will man sich an einem Vorbild orientieren: am Gemeinsamen Terrorismusabwehrzentrum (GTAZ) in Berlin. Ohne formalen Leiter, organisiert in verschiedenen Arbeitsgruppen, in denen unterschiedliche Behörden den Vorsitz führen, hat das GTAZ es offenbar geschafft, eine gute Zusammenarbeit zwischen zuvor mauernden oder auf ihre eigene Zuständigkeit bestehenden Polizei- und Geheimdienstbehörden zu organisieren.

BSI-Präsident Schönbohm und sein BKA-Kollege Münch gehören zu den Befürwortern eines solchen Cyber-GTAZ: Die Geschäftsführung würde danach wie bisher beim BSI bleiben, dessen ExpertInnen wären zuständig für Lagebeurteilung und technisches Know-how. Gestärkt würde vor allem die „operative Komponente". Notwendige Ermittlungen würde das BKA übernehmen; die Landeskriminalämter sollen eingebunden werden. Ebenso würde der Verfassungsschutz vorgehen; die Länder säßen mit am Tisch.

Bis heute gibt es keine gemeinsame Datenbank, in der Cybervorfälle registriert werden. Muster von Angriffen zu erkennen, um dann frühzeitig zu reagieren, macht dies fast unmöglich. Im Internet gibt es keine Staatsgrenzen, die Bedrohungen reichen von gewöhnlicher Kriminalität über Wirtschaftsspionage bis hin zur Bedrohung von Strom- und Wasserversorgung oder Atomkraftwerken. Eigentlich gibt es genau hierfür seit 2011 das Cyber-Abwehrzentrum in Bonn. Die dort eingesetzten ExpertInnen gelten als erstklassig, doch die Strukturen sind wenig befriedigend. Drei Jahre nach der Gründung kritisierte der Rechnungshof, das Konzept sei „nicht geeignet, die über die Behördenlandschaft verteilten Zuständigkeiten und Fähigkeiten bei der Abwehr von Angriffen aus dem Cyberraum zu bündeln".

Manche der dort eingesetzten Behörden schickten nicht einmal einen Vertreter zur täglichen Lagebesprechung. Kurz darauf kam der Auftrag für die Reform.

In internen Analysen heißt es, der für „den Staat, die Wirtschaft und die Bürgerinnen und Bürger erreichte Status quo" sei „nicht ausreichend". Als im Februar 2018 bekannt wurde, dass mutmaßlich russische Hacker in das Regierungsnetz eingedrungen waren, wusste das BSI Bescheid. Im Cyber-Abwehrzentrum aber war das am Tisch sitzende BKA nicht informiert worden. Dass sich nun eine Attacke gegen so viele PolitikerInnen gerichtet hat, löste im politischen Berlin Besorgnis aus. Manche SpitzenpolitikerInnen hatten über viele Jahre ihre Telefonnummern nicht gewechselt; dies wurde jetzt nötig. Der Ruf nach einer besseren Cyberabwehr ist laut.

Eine vom BKA eingesetzte Sonderkommission („Liste") ist nun dabei, die einzelnen Vorgänge nach ihrer Bedeutung zu gewichten. Die Länder wollten dem BKA nicht die alleinige Ermittlungskompetenz zugestehen. Alle Landeskriminalämter versehen die Fälle der Betroffenen mit einer Priorität. Wo der mutmaßliche Täter Johannes S. nur öffentlich zugängliche Daten sammelte und veröffentlichte, kommt für eine Strafverfolgung wohl „nur" ein Verstoß gegen das Datenschutzgesetz in Betracht. Die Ermittlungen konzentrieren sich auf die „ernsten Vorgänge", um die wegen des Verdachts des Ausspähens von Daten und der Datenhehlerei laufenden Ermittlungen voranzutreiben. Computer und Telefone könnten, sofern die Opfer zustimmen, forensisch untersucht werden.

Persönliche Konsequenzen

Den Bundesvorsitzenden von Bündnis 90/Die Grünen, Robert Habeck, hat es besonders getroffen: „Das ist, als wenn jemand in deinen Tagebüchern stöbert. Das zeigt auch, wie verletzlich wir sind." Er macht sich Sorgen um seine Familie: „Ständig klingelte das Telefon, das war wirklich nicht cool". Er teilte mit, dass er als eine Konsequenz auf den Datenklau seine Accounts auf Twitter und Facebook löscht. Einen Fehler könne man einmal machen, erklärt er nach einem von ihm als misslungenen bewerteten Eintrag auf Twitter; mit dem er eine vergleichbare Äußerung im Landtagswahlkampf in Bayern wiederholte: „Wie um alles in der Welt konnte mir so was passieren?" Bei seiner Analyse sei er zu dem Schluss gekommen, dass er sich jeweils „unbewusst auf die polemische Art von Twitter eingestellt habe". Twitter sei „wie kein anderes digitales Medium so aggressiv und in keinem anderen Medium gibt es so viel Hass, Böswilligkeit und Hetze". Offenbar werde auch er dadurch aggressiver, lauter und zugespitzter, ohne den Raum zum Nachdenken. Gleichzeitig desorientiere ihn der Kurznachrichtendienst und mache ihn unkonzentriert, wenn er dort nach Reaktionen auf seine Auftritte suche.

Eine Einstufung

- Doxing

Mit dem Hack wurde ein Begriff populär: Doxing (auch Doxxing, abgeleitete von „doc" Abkürzung für englisch „documents") ist das internetbasierte Zusammentragen und anschließende böswillige Veröffentlichen personenbezogener Daten. Eine Person veröffentlicht strategisch eine Sammlung privater Daten über einen Kontrahenten, vom bürgerlichen Namen über amtliche Dokumente bis zu Fotos und Chatverläufen und intimen Details. Mit dem aktuellen Veröffentlichen privater Daten von PolitikerInnen, Prominenten und JournalistInnen erreichte diese Hacker-Waffe endgültig den Mainstream. Vom Mittel der Wahl in privaten Fehden im Netz ist Doxing zur politischen Waffe geworden. Die digitalen Angreifer sammeln die Informationen aus öffentlichen Quellen, etwa per Google-Suche, in alten Foreneinträgen oder Archiven, in denen Webseiten zu verschiedenen Zeitpunkten gespeichert werden, aber auch mit Hacks gegen ungenügend gesicherte E-Mail- oder Social-Media-Konten. Die Daten veröffentlichen sie dann anonym oder pseudonym auf speziellen Upload-Diensten wie Pastebin. So liegen Teile des Privatlebens eines Menschen für alle zum Download bereit. Wer die Privatadresse einer Person kennt, kann ihr alles – von Pizza bis zu Sexspielzeug – liefern lassen. Wer ein intimes Bild hat, kann damit Pornofotomontagen basteln und verbreiten. Mit Kreditkartendaten lässt sich auf Kosten der Betroffenen einkaufen.

Opfer waren bisher besonders Frauen, vor allem, wenn sie sich für Frauenrechte einsetzten. Nach dem Hack ihres Dropbox-Kontos und anderer Accounts musste die amerikanische Spiele-Programmiererin Zoe Quinn 2014 monatelang eine organisierte Hasskampagne erdulden, die fast ihr Leben zerstörte. Die Frauenfeinde in der Gaming-Szene hatten zur Jagd auf sie geblasen. Nacktfotos aus Quinns zurückliegender Model-Karriere wurden verbreitet, ihr Telefon klingelte ständig, sie wurde nach eigenen Angaben mit Vergewaltigungsdrohungen überzogen.

Das BKA erklärte den betroffenen Bundestagsabgeordneten aus aktuellem Anlass in einem Schreiben: „Grundsätzlich stellt die Veröffentlichung von geleakten Listen kein Novum dar. Derartiges Vorgehen wird seit Jahren genutzt, nicht zuletzt um die betroffenen Personen zu verunsichern." So waren in den vergangenen Tagen auch AktivistInnen, die sich gegen Rechtsextremismus einsetzen, damit beschäftigt, die Verbreitung einer „schwarzen Liste" im Netz einzudämmen. Auf ihr stehen Namen, Adressen, Telefonnummern und E-Mails von mehr als zweihundert aktiven Personen. Manche Namen sind mit ausländerfeindlichen und homophoben Beleidigungen versehen und deuten darauf hin, dass Rechte die Liste hochgeladen haben. Auch die Namen von Teilnehmenden eines AfD-Parteitages landeten schon im Netz.

Doxing kann leicht zur Selbstjustiz werden. Das Hacker-Kollektiv Anonymous setzte die Taktik Mitte des vergangenen Jahrzehnts gegen Rechtsradikale und Pädophile und in ihrem Kreuzzug gegen Scientology ein. Und nach der Gewalt zwischen Neonazis und GegendemonstrantInnen in Charlottesville 2017 riefen Linke in den USA: „Dox a Nazi every day." Ihre Argumentation: Wer eine menschenverachtende Einstellung habe, der könne nicht auf Privatsphäre pochen.

Die AktionskünstlerInnen vom „Zentrum für politische Schönheit" spielten mit der Furcht vor dem digitalen Pranger, als sie 2018 auf einer Webseite vermeintlich Teilnehmende der Neona-



zi-Demo in Chemnitz enthüllten. Kurz darauf stellten sie die Aktion allerdings als Falle dar: Sie hätten kaum selbst Informationen gehabt, sondern hätten nur die Namen jener Rechten abgreifen wollen, die nun panisch auf der Webseite des „Zentrums“ nach sich selbst suchten.

In rechten Foren kursieren Kontaktlisten angeblicher Mitglieder der Antifa. Kurz nach Bekanntwerden des Promi-Doxings wurden dort 200 Namen und Adressen von PolitikerInnen, KünstlerInnen und AktivistInnen, die für eine liberale Haltung in der Flüchtlingsfrage stehen, unter dem Motto „Wir kriegen Euch alle“ veröffentlicht.

- Schlimm? Was tun?

Laut einer repräsentativen Umfrage des Branchenverbands Bitkom war im Jahr 2018 jeder zweite Internetnutzende Opfer von Cyberkriminellen. Am häufigsten klagten die Betroffenen über die illegale Verwendung ihrer persönlichen Daten oder die Weitergabe der Daten an Dritte. Die meisten Menschen bewerten Daten- und Identitätsklau nach Einschätzung von Sven Herpig von der Stiftung Neue Verantwortung als „Kavaliersdelikt“: „Die wenigsten begreifen es als eine Straftat, die man anzeigen sollte.“

Wer gedoxt wird, kann versuchen, die Plattformen zu informieren, auf denen das Material aufgetaucht ist. Seit 2015 können Nutzer auf Twitter das „Posten von privaten und vertraulichen Informationen anderer Personen“ als Missbrauch melden und zumindest auf eine schnelle Reaktion des Netzwerks hoffen. Zahlen gibt das Unternehmen bisher auch auf Anfrage nicht heraus.

Richtig ist – wenn ein Cyberangriff über das für Internetuser täglich übliche Maß hinausgeht – das Informieren der Polizei. Dabei sollten die elektronischen Spuren so gesichert werden, dass sie keinen weiteren Schaden anrichten können, und an die Polizei weitergegeben werden. Bestehen valide Ansätze für eine Zuordnung einer Verantwortlichkeit für einen Angriff, so sollte in jedem Fall auch die zuständige Datenschutzaufsicht eingeschaltet werden und zudem über sonstige Maßnahmen, insbesondere auch die Einschaltung der Strafverfolgungsbehörden nachgedacht werden.

Wegen der Massenhaftigkeit von Cyberkriminalität wie Identitätsklau und Rufschädigungen im Netz ist es für staatliche Stellen derzeit und absehbar objektiv nicht möglich, alle versuchten Angriffe zu verfolgen, geschweige denn aufzuklären. Daher hat Selbstschutz im Netz und insbesondere bei Social Media Priorität. Auch wenn es keine hundertprozentige Sicherheit gibt, sollten folgende Maßnahmen für jede UserIn in Fleisch und Blut übergehen: Bei jeder E-Mail muss der Absender und der Inhalt gecheckt werden, bevor z. B. Anhänge geöffnet werden. Bei Unplausibilitäten ist im Zweifel eine Rückversicherung nötig; dubiose Mails sollten umgehend gelöscht, dubiose Webseiten sollten umgehend verlassen werden. Wer Anlass zur Annahme hat, dass sein E-Mail-Konto gehackt wurde, kann über Identity-Checker versuchen mehr Klarheit zu bekommen (z. B. https://sec.hpi.de/ilc/ oder haveibeenpwned.com). Passwörter sollten mindestens zehnstellig sein, unplausible Zeichenfolgen enthalten und sich für jedes Konto unterscheiden. Zumindest bei sensiblen Inhalten ist eine Zwei-Faktor-Authentifizierung dringend zu empfehlen. Bei der Speicherung ist eine Verschlüsselung geboten; ebenso bei der Versendung von sensiblen E-Mails. Der weit verbreitete, bisher offenbar nicht kompromittierte Standard ist Pretty Good Privacy (PGP). Bei Messengerdiensten sollte man gemeinsam mit seinen KommunikationspartnerInnen nur solche nutzen, die eine Ende-zu-Ende-Verschlüsselung vorsehen. Regelmäßige Datensicherungen auf einem eigenen Datenträger sind zuverlässiger als die Nutzung von Clouddiensten. (Zumeist unentgeltliche) Dienste aus dem Ausland, insbesondere aus den USA und China, für die Teil des Geschäftsmodells die Nutzung der personenbezogenen Daten sind, sollten gemieden werden. Das gilt etwa auch für Twitter, Facebook oder WhatsApp.

- Wo bleibt der Datenschutz?

Das Doxing gegen deutsche Prominente ist nun Anlass, sich verstärkt über den Persönlichkeitsschutz im Internet Gedanken zu machen. Der Vorgang selbst weist schon auf eine problematische Tendenz hin: Doxing ist nichts anderes als eine besonders gravierende Datenschutzverletzung. In der öffentli-

chen Debatte um den Promi-Hack waren aber die unabhängigen Datenschutzaufsichtsbehörden nicht präsent. Dies mag auch daran gelegen haben, dass es die bisherige Bundesbeauftragte nicht als ihre Aufgabe ansah, auf derartige Vorgänge adäquat zu reagieren. Dies wird hoffentlich bei ihrem Nachfolger besser werden. Das Ausblenden der unabhängigen Datenschutzaufsicht war zugleich kein schlechter medialer Schachzug des Bundesinnenministers, der sein BKA und sein – eigentlich unzuständiges – BSI in den Vordergrund schob. Seehofer will – im Interesse der Zugriffsmöglichkeit seiner Sicherheitsbehörden auf private Daten – nicht mehr Selbstschutz und mehr von den Anbietern eingebaute Datensicherheit. Solange er die mediale Hoheit über solche Themen behält, wird es schwer sein, insofern politisch weiterzukommen.

Verwendete Quellen: Bünte, Hackerangriff: Persönliche Dokumente von deutschen Politikern und Promis veröffentlicht, www.heise.de 04.01.2019; Scherschel, Politiker- und Promi-Hack: Ehemaliges Twitter-Konto eines YouTubers missbraucht, www.heise.de 04.01.2019; Krempl, Gehackte Daten: Politiker beklagen schweren Angriff auf die Demokratie, www.heise.de 04.01.2019; Krempl, Massen-Doxxing: Datenschützer will Twitter zum Sperren von Links verpflichten, www.heise.de 05.01.2019; Hackerangriff: BSI wusste schon länger vom Datenleck – das BKA nicht, www.heise.de 05.01.2019; Hanauer, Datenleck trifft viele Politiker aus Schleswig-Holstein, Kieler Nachrichten, 05.01.2019, 1; Köpke, Unser geleaktes Heimatland, Kieler Nachrichten 05.01.2019, 3; Anzlinger/von Billion/Hurtz/Tandriverdi, Daten Hunderter Politiker gestohlen, SZ 05./06.01.2019, 1; Unionsfraktionschef für höheres Strafmaß bei Datendiebstahl, www.heise.de; Holland, Nach Datenklau und Twitter-Malheur: Grünen-Chef verlässt Twitter und Facebook, www.heise.de 07.01.2019; Brühl/Fried/Höll, Das Beben aus dem Kinderzimmer, SZ 09.01.2019, 5; Fried/Höll, Ein Schüler stahl die Politiker-Daten, SZ 09.01.2019, 1; Brühl, Der digitale Pranger, SZ 09.01.2019, 9; Hurtz/Steinke, Tandriverdi, Quälgeister, SZ 08.01.2019, 2; Scherschel, Massen-Doxxing: Täter hat sich wohl schon 2016 verraten www.heise.de 10.01.2019; Amann/Baumgärtner/Bohr/Diehl/Gebauer/Höfner/Knobbe/Lehberger/Medick/Müller/Pauly/Rosenbach/Seibt/Wiedmann-Schmidt, Plötzlich nackt, Der Spiegel Nr. 3 12.01.2019, 15-23; Telekom: Datendiebstahl strenger bestrafen, www.heise.de 13.01.2019; Massen-Doxxing: Barley hält Musterklage gegen Internetkonzerne für denkbar, www.heise.de 13.01.2019; Mascolo, Die Wacht am Rhein soll aufwachen, SZ 17.01.2019, 6.

Katrin Lowitz

beyond-EVE – Eine alternative Social-Media-Plattform

Als Christopher Wylie im März 2018 mit seinen Informationen über Cambridge Analytica an die Öffentlichkeit ging, hatte ich bereits ein Jahr Bemühungen hinter mir, eine schnelle Alternative für eine zweckgerichtete Netzwerkplattform aufzubauen, die Menschen und Organisationen schneller verbinden kann als die KI-getriebenen Plattformen der sozialen Medien. Die Intention meiner Plattform beyond-EVE (Encounter, Values, Environment) ist es, die Hoheit über den Zugang zu relevanten Informationen wieder an die User zurück zu geben im Sinne eines Lean Networking: Zeige in 5 Minuten ein Thema aus einer 360°-Perspektive aus Politik, Unternehmen und Zivilorganisationen.

Nochmal einen Schritt zurück: Februar 2017, US-Präsident Trump war vereidigt. Die ersten verstörenden Amtshandlungen schickten bereits Schockwellen durch die geopolitische Welt. Der US-Wahlkampf 2016, der von allen Beteiligten intensiv auch über die sozialen Medien gespielt worden war, war gelaufen, mit einem unwirklichen Ergebnis. Im Dezember 2016 wurde bereits darüber diskutiert, welche Einflussnahme die sozialen Medien wohl auf den Wahlkampf hatten.

Im gleichen Zeitraum 2016 hatte ich als Vertreterin einer ehrenamtlichen Organisation intensiv zu Öffentlichkeitsarbeit recherchiert. „Social-Media-Marketing muss man machen“, hieß es, daran führe kein Weg vorbei. Also, es funktioniert so:

1. Ständig online sein, posten und teilen. Nur wer seine Mitmenschen mit ständigen Botschaften bearbeitet, wird wahrgenommen.
2. Aufmerksamkeit generieren durch Likes und Kommentare bei Anderen; am besten mit einem knalligen Spruch, bloß nicht zu viel Inhalt.
3. Mit Geld für die Plattformbetreiber sind zielgenau bestimmte Gruppen anzusprechen. Alter, politische Ausrichtung, Einkommensverhältnisse, Interesse, Hobbys wurden bereits vom Plattformbetreiber ausgespäht, so dass meine Botschaft zielgerichtet einschlägt.
4. Der Algorithmus spült meine Werbung Anderen in die Timeline. Die Opfer meiner Bemühungen arbeiten sich durch die Werbepost. Da es alle so machen und die Aufmerksamkeitsspanne der Zielpersonen trotzdem nicht größer wird, kleben alle ewig an ihrem Smartphone (Attention Economy heißt das).
5. Alle sind im Sendemodus, Hauptsache: Posten und weg, Daumen hoch, Herzchen …
6. Inhalte sind zu 85% belanglos, zu 5% Hass, zu 10% interessant. Wie bekomme ich nur diese 10%?
7. Seriöse Medien heben das Niveau durch ihre Beiträge und veredeln dadurch die Plattformen.

Ich versuchte es ein paar Monate. Aber es nervte, es kostete viel zu viel Zeit. Ich beobachtete das Bemühen anderer Zivilorganisationen, die für ihre Themen ebenfalls im Verhältnis wenig Rückkopplungen bekamen. Ich beobachtete, wie mich die „Filterblase" einkreiste. Ich agierte in meinem Themengebiet und das Dopamin im Hirn belohnte mich, wenn jemand meine Beiträge mochte. Für wen arbeitete ich hier eigentlich?

Das Ergebnis meiner Untersuchung ist: Die Plattformen wollen

1. Lange online-Zeiten der User.
2. Analyse der User durch Beobachtung, was angeklickt wird.
3. Konsum-orientierte Werbung verkaufen. Wer zahlt, wird gezeigt!
4. Social Media wird damit zum Konsumturbo.
5. Non-Profit-Organisationen, Forschung, Bildung werden äußerst nachrangig und sind nicht gut zu finden.
6. Der Nebennutzen: Sicherheitsbehörden von undemokratischen und demokratischen Ländern haben ein perfektes Überwachungsinstrument.

Dann im Februar 2017 sah ich das: Alexander Nix von Cambridge Analytica (CA) stellt einem interessierten Publikum im September 2016 auf der Konferenz Concordia in New-York vor, wie Microtargeting im Wahlkampf von Ted Cruz/Trump lief. Bei YouTube unter „Cambridge Analytica - The Power of Big Data and Psychographics" wurde es erläutert. Erschütternd aber: Egal ob die Befähigung von CA nun da war oder nicht, alle hätten gerne dieses Instrument, denn damit ist viel Geld zu machen. Also, dieses ständige Suchen ist nicht das Arbeitsergebnis eines schlechten Programmierers, sondern eine bewusste Manipulation, um die Menschen vor ihren Geräten zu halten, damit sie ausspioniert werden können. Jeder Klick liefert eine Information an den Plattformbetreiber, die monetarisiert wird.

Wie würde eine bessere Plattform aussehen, die innerhalb von 5 Minuten relevante Informationen sortiert? Dazu müsste definiert werden, was relevant ist. „Open and connected", das Credo von Mr. Zuckerberg, ist ein bisschen wenig. Facebook ist nun seit einem Jahr in der Beobachtung der Öffentlichkeit und hält mehr Fragen offen, als dass sie Antworten liefern.

Nach verschiedenen Umwegen seit März 2017 und auch aufgrund der Brisanz der globalen Entwicklung ist die Agenda 2030 mit den 17 Nachhaltigkeitszielen der UN, die von fast allen Staaten anerkannt wurden, der Rahmen für die Beteiligung bei beyond-EVE (Encounter, Values, Environment). Die Ziele sind transparent und für alle nachvollziehbar. Hiermit ist das gesamte Wirtschaftssystem, sowie Forschung, Bildung, Gesundheit und Innovationen über alle Industriebereiche abgedeckt. Inzwischen haben fast alle wirtschaftlichen Aktivitäten Einfluss auf die Nachhaltigkeitsziele. Wirtschaftliche Aktivitäten und politische Regularien werden sich mehr und mehr an diesen Zielen ausrichten.

Welche Plattformbedingungen sind erforderlich?

1. Ergebnisse sollen innerhalb von 5 Minuten gefunden werden.
2. Keine Profile von Privatpersonen; dies würde wieder zu Datenschutzproblemen führen und wiederum die Menge an Einträgen unnötig vervielfachen; anonyme Konten sind nicht verifizierbar bei Falschmeldungen; verifizierte Konten führen wieder zu Überwachungspotentialen.
3. Profile können nur von Organisationen angemeldet werden.
4. Keine Likes und Kommentare; alle Plattformen, deren positive Kommentare zu wirtschaftlichem Erfolg führen, haben langfristig Probleme mit unehrlichen oder gekauften Klicks oder manipulierten Einträgen.
5. Kein Ranking nach Menge, denn vielleicht hat gerade die kleinste Organisation die beste Idee oder das beste Angebot.
6. Niemanden auf der Plattform festhalten; wenn ein Ergebnis gefunden wurde, direkt zum digitalen oder analogen Ziel weiterleiten. Schnell ein Ergebnis zu liefern ist unser Ziel.

Die Profileinträge der Organisationen sollen auf das Wesentliche beschränkt werden:

- Wer ist die Organisation?
- Was sind die Arbeitsergebnisse?
- Welche Veranstaltungen, Angebote, Produkte liefern sie?
- Wie können sich Interessierte offline beteiligen?
- Anbieter von Informationen sollen möglichst wenig Aufwand mit dem Einstellen haben.
- Hoch-individualisierte Tags werden nicht zugelassen, denn sie erschweren nur die Ergebnisfindung.
- Filter werden mit Umfang der Plattform verfeinert.
- Für Privatpersonen gibt es keine Barrieren, um sich anzumelden; die Informationen stehen offen zur Verfügung.
- Niemand soll gezwungen werden seine persönlichen Daten anzugeben, um an Informationen zu kommen.
- Non-Profit-Organisationen können kostenlos Angebote einstellen.

In der Planung sind weitere Ausbaustufen; auch eine interaktive personenbezogene Aktionsplattform ist noch in der Konzeption. Allerdings sehe ich derzeit keine Möglichkeit, dass sich Personen anonym anmelden können, wenn die Qualität gehalten werden soll. Dies würde zu den gleichen Problemen führen, mit denen sich die Plattformbetreiber schon jetzt herumschlagen.

Es gäbe interessante Themen und engagierte Organisationen und Möglichkeiten sich analog wieder mehr zu treffen, wenn man sie denn finden würde. Das ist unser Ziel, hierbei wollen wir die vielen Organisationen und Unternehmen unterstützen, ihr Angebot einem größeren Publikum vorzustellen und Filterblasen zu beenden. Privatpersonen sollen wieder die Informationsflut beherrschen können, nicht stundenlang suchen müssen. Sie sollen keine tolle Veranstaltung mehr verpassen; sie sollen Bildungsangebote finden. Und über Themen wie z.B. Mobilität oder Digitalisierung sollen sie eine 360°-Sicht aus den unterschiedlichsten Perspektiven bekommen.

Die analoge Interaktion zwischen den Menschen kann mit dem besseren Zugang zu Veranstaltungen und Beteiligung wieder in einem sozialen, interaktiven Umfeld geführt werden. In einer Diskussion zuhören, seine eigene Meinung vertreten, sich die Antworten anhören und in weitere Diskussion treten: Hierzu wollen wir unseren Beitrag leisten.

Heinz Alenfelder

Twitter und Datenschutz – Ein Überblick

Die großen Player im Bereich der Sozialen Medien wie Facebook und Google stehen schon lange in der Kritik, werden aber dennoch fortwährend genutzt. Twitter ist zumindest in Deutschland zwar eher unwichtig, scheint jedoch durch @realDonaldTrump mit seinen 40.000 Tweets und 57 Millionen Follower weltweit geadelt zu werden. Dieser Beitrag soll zeigen, wie es in diesem Feld der permanenten freiwilligen Veröffentlichung mit dem Datenschutz aussieht, dem Schutz personenbezogener Daten an sich und den Möglichkeiten von Datenauswertungen. Abschließend wird ein Blick auf Stellungnahmen von Datenschutz-Behörden geworfen. Damit soll auch eine Berichtslücke der DANA geschlossen werden, denn Twitter findet seit 2010 nur sporadisch in DANA-Beiträgen Erwähnung.

DANA-Beiträge mit Erwähnung von Twitter

Heft/Seite	Beitragstitel
2015-1/46	Twitter spioniert Apps aus
2014-2/83	Twitter kauft Datenauswerter Gnip
2012-3/122	SPD-Nutzerdaten gehackt
2011-4/176	Netzkontrolle nach Unruhen - „Überwachen statt abschalten“
2011-3/127f	Mann zur Twitterentschuldigung gerichtlich verpflichtet
2011-1/24	Polizeichefin wegen voreiligem Twittern suspendiert
2011-1/28	USA - Regierung fordert Personendaten von Twitter
2011-1/4f	Grenzen der digitalen Anonymität
2010-3/101	Geolokalisierung und Geotracking – Herausforderungen für Location Privacy
2010-1/10	Wenn das Smartphone (nicht nur) nach Hause telefoniert

Begrifflichkeiten bei Twitter

Zunächst sei knapp zusammengefasst, wie die Funktionsweise des Kurznachrichtendienstes Twitter aussieht. Übliche Vorgehensweise ist die einmalige Registrierung unter einem Twitter-Namen, die auch mit Pseudonym möglich ist. Diese Personen/Accounts werden innerhalb von Twitter mit einem vorangestellten „@“-Zeichen gekennzeichnet. Nach der Anmeldung können Text-Nachrichten (Tweets) mit bis zu 280 Zeichen sowie Fotos und Videos versendet werden. Das Weiterleiten eines nicht selbst geschriebenen Tweets heißt Retweet. Der Abruf von Tweets ist zwar auch ohne Anmeldung möglich (eine Suche erfolgt zum Beispiel mit https://twitter.com/search?q=datenschutz), aber die folgenden Erläuterungen beziehen sich auf die Situation nach einer Anmeldung im Webbrowser (www.twitter.com).

Die Twitter-Startseite zeigt nach der Anmeldung im Fokus chronologisch geordnet Tweets und Retweets derjenigen Personen an, denen der/die Angemeldete „folgt“ (d. h. als deren Follower sie sich hat registrieren lassen). Das „Folgen“ ist Basis für den Aufbau einer Sphäre von Twitter-Accounts, in denen sich meist Gleichgesinnte vernetzen, die dieselben Interessen haben. Von Zeit zu Zeit wird die beim Anmelden gezeigte Abfolge von Tweets durch Empfehlungen und Werbe-Tweets unterbrochen. Followern können Direktnachrichten gesendet werden, die nicht öffentlich einsehbar sind.

Innerhalb des Dienstes kann nach Stichworten in den Tweets und in den Beschreibungen von Fotos, Videos oder auch Personen gesucht werden. Bei der Suche werden standardmäßig „Top“-Tweets gezeigt; möglich ist die Sortierung nach Datum („Neueste“). In derselben Ansicht kann die Suche per „Suchfilter“ durch Datums-, Orts- oder Personen-Angaben erweitert werden. Zum Hervorheben und als spätere Sucherleichterung können wichtige Worte in einem Tweet mit einem führenden Raute-Zeichen (#) versehen werden, was dann zu den sogenannten Hashtags führt, die heutzutage auch in anderen Zusammenhängen als Kennzeichnung verwendet werden (Beispiel: #Datenschutz).

Sowohl auf der allgemeinen Startseite nach der Anmeldung als auch in

der Such-Ergebnisseite schlägt Twitter „Wem folgen?“ und „Trends für dich“ vor und macht so maßgeschneiderte Vorschläge für Accounts und Tweets, die vermeintlich den eigenen Interessen am nächsten kommen. Ein „Ändern“ ermöglicht die Angabe eines anderen Ortes, wobei unklar bleibt, ob weitere Nutzungskriterien zur Anzeige von Tweets aus dieser Stadt/diesem Land hinzugezogen werden.

Bei Gefallen kann ein Tweet durch das Anklicken eines Herzsymbols „gelikt“ werden (eingedeutscht vom englischen Verb „to like“). Die Zahl der „Likes“ führt offensichtlich zu einer höheren Position bei den „Top“-Tweets.

Die Twitter-Datenschutzrichtlinie – Alles für die Werbung?!

Im Folgenden werden wichtige Punkte aus der 14-seitigen Twitter-Datenschutzrichtlinie[1] vom 25. Mai 2018 zusammengefasst. Alle Zitate sind diesem Dokument entnommen. Ein Blick auf den Vorspann der Datenschutzrichtlinie zeigt als Kernpunkte die generelle Öffentlichkeit aller Tweets und die Tatsache, dass Daten auch bei unangemeldeter Nutzung anfallen. Informationen, die über das technisch Notwendige hinausgehen, werden genutzt „für Dinge wie die Sicherheit Ihres Accounts und um Ihnen relevantere Tweets, Personen, denen Sie folgen können, und Anzeigen anzuzeigen“. Dann wird offengelegt, dass zusätzlich zu den mit Anderen geteilten Informationen sämtliche Tweets (gelesene, gelikte und auch retweetete) „sowie weitere Informationen“ genutzt werden, um Interessensgebiete, Alter, Sprachen sowie „weitere Signale“ zu bestimmen. Schon an dieser Stelle muss auf die Gefahren der Auswertung von Big Data hingewiesen werden.

Zu den grundlegenden Accountdaten gehören

- ein angezeigter Name,
- der Nutzer-/Nutzerinnen-Name,
- Passwort,
- E-Mail-Adresse oder Telefonnummer.

Öffentlich sind

- Profilangaben,
- Zeitzone und Sprache,
- Datum der Account-Erstellung,
- die Tweets und dazu
  - Datum,
  - Uhrzeit sowie die
  - Applikation, mit der sie erstellt wurden.

Die Ortsangaben in Tweets können abgestellt werden. Des Weiteren einsehbar sind die Follower sowie die „Gefällt mir“-Angaben. Außerdem stellt die Richtlinie klar: „Informationen, die andere Personen, die unsere Dienste nutzen, über Sie veröffentlicht haben, können auch öffentlich sein. Zum Beispiel können andere Personen Sie in einem Foto markieren (falls Ihre Einstellungen dies erlauben) oder in einem Tweet erwähnen.“

Twitter ist durchaus zugute zu halten, dass immer wieder Hinweise in den Erklärungen erfolgen, die zum bewussten Umgang mit Daten aufrufen. Ein Beispiel dazu: „Sie sind verantwortlich für Ihre Tweets und andere Informationen, die Sie über unsere Dienste angeben, und Sie sollten sorgfältig darüber nachdenken, was Sie öffentlich machen, insbesondere dann, wenn es sich um sensible Informationen handelt“. Weniger klar ist die Erklärung, wie die Daten genutzt werden. Natürlich dienen die Accountdaten der Authentifizierung. Darüber hinaus weist die Datenschutzrichtlinie aber immer wieder auf Twitter-„Dienste“ hin, bezüglich derer es sowohl eine Vielzahl von Einstellungen als auch eine nicht näher genannte Zahl von „verbundenen Unternehmen“ gibt. Die Dienste dienen wohl vor allem zur Zusendung von Werbung per E-Mail und SMS. Beim Hochladen des gesamten Adressbuchs eines Smartphones nutzt Twitter die Kontaktdaten „auch, um Ihnen und anderen besser Inhalte empfehlen zu können“.

Auch die Direktnachrichten, die nicht öffentlich nur an Ausgewählte gerichtet sind, werden von Twitter gescannt, um „bösartige Links“ zu finden und „Spam und verbotene Bilder“ aufzudecken. Zwar werden die Inhalte dieser Direktnachrichten nicht für Anzeigen benutzt, allerdings begründet Twitter das Speichern und Verarbeiten von Metadaten auch damit, „relevantere Inhalte“ anzeigen zu wollen, und betont lediglich: „Wir nutzen auch Informationen darüber, mit wem Sie kommuniziert haben und wann (aber nicht die Inhalte dieser Kommunikationen)“.

Eine vierseitige Beschreibung von „zusätzlichen Informationen“ enthält Erläuterungen zu Standortdaten, aufgerufenen Links in Tweets und E-Mails sowie temporär und dauerhaft gesetzten Cookies, mit denen Nutzungsdaten gesammelt werden. Twitter unterstützt nicht die „Do Not Track“-Browseroption. Auch ohne Anmeldung sammelt Twitter Informationen, „wenn Sie Inhalte ansehen oder unsere Dienste anderweitig nutzen“ und bezeichnet sie als „Log-Daten“. Die maximal 18 Monate aufbewahrte Liste von Log-Daten ist erklecklich:

- IP-Adresse
- Browsertyp
- Betriebssystem
- Informationen zu der zuvor aufgerufenen Website und den aufgerufenen Seiten
- Standort
- Mobilfunkanbieter
- Geräteinformationen (einschließlich Geräte-ID und Anwendungs-ID)
- Suchbegriffe
- Cookie-Informationen

Bezüglich der Nutzung dieser Daten wird wieder in einem Atemzug sowohl die Account-Sicherheit als auch die Werbung genannt: Twitter interessiert sich dafür, „welche Inhalte in unseren Diensten beliebt sind“ und benutzt die Daten, um „Schlussfolgerungen zu ziehen z. B. darüber, an welchen Themen Sie interessiert sein könnten, wie alt Sie sind und welche Sprachen Sie sprechen“.

Zusätzlich taucht immer wieder der Begriff der „relevanteren Inhalte“ auf, hinter dem die Werbung steckt, die letzten Endes auch geräteübergreifend ausgespielt wird: „Besuchen Sie zum Beispiel Websites mit Sport-Inhalten über Ihren Laptop, können wir Ihnen sport-bezogene Anzeigen auf Twitter für Android zeigen.“ Twitter zeigt mit der umfangreichen Datenschutzrichtlinie auf, dass Transparenz, wie sie von der DSGVO gefordert wird, ähnlich wie der Begriff der Schönheit, im Auge des Betrachters liegt. In der alltäglichen Nutzung des Twitter-Accounts mit Nachrichten, Kommentaren, Likes und Fotografien von Kleidung, Mahlzeiten, Landschaften und Personen gewinnen Formulierungen wie „relevantere Inhalte“ eine neue Bedeutung.

Natürlich lässt Twitter eine ganze Reihe von Einstellungen zu, allen voran das

Abstellen der Ortsangabe in Tweets. Hier soll lediglich das Augenmerk auf die „Personalisierung" gerichtet werden, die ausschlaggebend für die auf Twitter angezeigte Werbung ist. Basis der ausgelieferten Anzeigen ist die Twitter-Aktivität, mit der „Anzeigen auf Twitter und anderswo durch Kombination deiner weiteren Online-Aktivitäten" personalisiert werden. Die entsprechende Auswertung von Twitter bezieht sich auf alle Geräte, auf denen die Nutzenden sich anmelden. Weiter hinzugezogen werden „Drittanbieter-Websites mit integrierten Twitter-Inhalten oder auch von Twitter aus besuchte Werbekunden". Schließlich werden der aktuelle und frühere Standorte für die Personalisierung von Anzeigen ausgewertet.

Entlarvend sind schließlich die Erklärungen zu Zielgruppen. Nebulös wird erklärt, dass Werbekunden Twitter-Nutzende aus „E-Mail-Listen oder basierend auf dem Browserverhalten" in maßgeschneiderte Zielgruppen aufnehmen. Twitter selbst hat dann ebenso Zielgruppen aufgebaut, indem die „Ähnlichkeiten zwischen deinem Account und den Accounts [...], die in maßgeschneiderten Zielgruppen enthalten sind" ausgewertet wurden. Die Einstellungen erlauben, sich aus diesen Zielgruppen und von „weiterer interessenbasierter Werbung" abzumelden. Ein glatter Hohn wird das angesichts der ausdrücklichen Betonung seitens Twitter: „Durch Ändern der Einstellung siehst du andere Anzeigen auf Twitter, du wirst jedoch nicht aus diesen Zielgruppen entfernt."

Auswertung von Twitter-Daten – Grenzenlose Nutzung

Die folgende kleine Stichprobensammlung soll nun zeigen, wer außer Twitter die Daten des Micro-Blogging-Dienstes noch nutzt bzw. nutzen möchte. Werbung ist nämlich die eine Seite der Medaille, doch andererseits steht Twitter auch für die Big-Data-Auswertung. Sie ermöglicht beispielsweise das Microtargeting, bei dem Datenanalysen genutzt werden können, um Wählergruppen oder auch sogar einzelne Wähler und Wählerinnen gezielt anzusprechen. Papakyriakopoulos und andere haben in einer Analyse von Facebook-Daten[2] herausgearbeitet, dass „es im Einklang mit den deutschen Datenschutzgesetzen möglich ist, Daten aus dem sozialen Netzwerk Facebook zu extrahieren und damit Microtargeting zu betreiben". Sie werteten dazu die „Likes" der Nutzerinnen und Nutzer zu politischen Posts aller großen Parteien aus. „Auf Basis von standardisierten Microtargeting-Auswertungsmethoden konzentrieren wir uns bei der Auswertung auf Nutzer, die Inhalte auf Seiten von unterschiedlichen Parteien ‚gelikt' haben." Auf diese Weise wurden mögliche Wechselwähler im Umfang von ca. 20 Prozent identifiziert. In Kombination mit anderen Interessengebieten kommen laut Aussage der Autoren Informationen zusammen, die „für einen geübten Wahlkämpfer bereits [reichen], um eine sehr persönlich wirkende Ansprache zu verfassen und dem Nutzer personalisierte Wahlwerbung zu senden." Analog dürfte das für Twitterdaten gelten.

Ein konkretes Beispiel dafür, wie Twitterdaten genutzt werden können, ist ein Projekt der Stiftung Mercator am Marburger Centrum für Nah- und Mittelost-Studien (CNMS)[3]. Aufgrund bisher fehlender Sekundärliteratur zum Thema Atheismus in der Türkei wird in diesem Projekt, an dem auch Wissenschaftler zweier Istanbuler Hochschulen beteiligt sind, Twitter herangezogen. Der projektleitende Islamwissenschaftler Pierre Hecker: „Das Projektteam analysiert den öffentlichen Diskurs um Atheismus unter anderem über eine systematische Auswertung von Twitter-Daten".

Nicht nur für nachträgliche Auswertung, sondern auch für akute Situationen ist Twitter als Datenquelle hervorragend geeignet. Auf der deutschen Webseite der Österreichischen Zeitung „Der Standard" berichtet Katharina Kropshofer am 17.8.2018 über ein Dissertationsprojekt[4]. Cornelia Ferner, Institut für Informationstechnik und Systemmanagement an der Fachhochschule Salzburg, will Tweets über Katastrophenfälle auswerten: „Auf Twitter sind Daten in Echtzeit vorhanden. Bei Naturkatastrophen kann das eine wertvolle Informationsquelle sein". Dass mit einer solchen Methode auch im Alltag beliebige Analysen durchgeführt werden können, wird durch folgende, weit verbreitete Ansicht deutlich: „Im Bereich Data-Science sind die Algorithmen, die man verwendet, eigentlich immer die gleichen. Die Inhalte, die man reinsteckt, sind dem Algorithmus egal".

Fabian Pfaffenberger schließlich schätzt 2016 in seiner Masterarbeit „Twitter als Basis wissenschaftlicher Studien"[5] den Datenpool von Twitter auch deshalb als sehr interessant ein, weil bei dessen Nutzung, „(zunächst) keine strengen Datenschutz- und Anonymisierungsauflagen" zu erfüllen seien. Er gelangt allerdings zu der Einschätzung, dass die Erkennung von Propaganda und Spam in Tweets eine Herausforderung ist, die vor der Nutzung für wissenschaftliche Analysen bewältigt werden muss. Außerdem fehlten für Studien über Tweets die Repräsentativität und der kommunikative Zusammenhang. Hinzu kämen natürlich die Kosten, die bei Nutzung des exklusiven Datenlieferanten Gnit entstehen. Nicht nur dieser Autor sieht bei allen Hindernissen zahlreiche Einsatzgebiete: „Von der Echtzeit-Erkennung von Epidemien oder Unglücken über die Stimmungsanalyse während medialer Großereignisse bis zur Erstellung von Bewegungsprofilen, Stimmungsverläufen oder Interaktionen ausgewählter Nutzer".

Weitere Gefahren durch Twitter

Ob nun die Nutzung von Twitter-Daten im Wahlkampf zwecks Microtargeting oder zu diversen Studienzwecken, eine Betrachtung weiterer Veröffentlichungen zeigt, dass noch ungeahnte Gefahren lauern können. So stellen Czech, Podoll und Schneider in ihrem Beitrag in der Zeitschrift „Der Nervenarzt"[6] fest, es sei „auf vielen psychiatrisch-psychotherapeutischen und psychosomatischen Stationen inzwischen alltägliche Praxis, dass Patienten auf eigene Initiative untereinander per Messenger kommunizieren, sowohl in Einzel- als auch und vor allem in Gruppenchats". Sie sehen Regelungsbedarf bezüglich Restriktionen im therapeutischen Setting und zur Verhinderung von strafbaren Handlungen und konstatieren: „Insbesondere bezüglich möglicher auch positiver Wirkungen von Gruppenchats besteht weiterer Forschungsbedarf". Als praktischen Hinweis heben sie die „Leitlinien für die Nutzung sozialer Netzwerke für Krankenschwestern und -pfleger" hervor, die 2012 in Amerika implementiert wurden.

Bereits 2014 hat Jalal Mahmud am IBM Research Center herausgefunden, dass 200 Tweets eines Nutzers reichen, um eine Ortsbestimmung vorzunehmen, auch ohne dass diese Information in den Tweets freigeschaltet wäre. In einer Studie[7] wertete er mit seinem Team die Inhalte von ca. 1,5 Millionen US-amerikanischer Tweets aus, die mit Geotags gekennzeichnet waren. Die Forschungsgruppe trainierte den Algorithmus und konnte dann bei Tests zu über zwei Dritteln der Tweets den korrekten Wohnort und Bundesstaat ermitteln. Das Feststellen der Zeitzone gelang sogar bei 80 Prozent der Testtweets. In den Folgejahren analysierte Mahmud jeweils mit seinem Team Themen wie „Predicting attitude and actions of twitter users“[8] oder „25 Tweets to Know You“[9]. Bei der letzten Studie von 2017 handelt es sich um ein Modell zur Vorhersage von Persönlichkeitseigenschaften mit Social Media.

Äußerungen einschlägiger Behörden zu Twitter

Auf der Suche nach Informationen ist es naheliegend, die Webseiten von Institutionen anzusteuern, die sich mit dem Datenschutz befassen und für die Aufsicht zuständig sind. Die folgende Übersicht soll durch ihre Reihenfolge keine Bewertung darstellen, sondern als Überblick zeigen, dass die Informationsflut hier eher spärlich sickert.

Düsseldorfer Kreis[10]

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) fassten zuletzt in 2011 einen Beschluss zum Datenschutz in sozialen Netzwerken. Damals gingen sie auf die Selbstverpflichtungen der Netzwerkbetreiber ein, begrüßten sie als „Schritt in die richtige Richtung“ und stellten fest, dass das deutsche Datenschutzrecht nur unter ganz bestimmten Bedingungen nicht zu Geltung kommt. Zur Wahrung des Rechts auf informationelle Selbstbestimmung forderten sie „leicht zugängliche und verständliche Information darüber [...], welche Daten erhoben und für welche Zwecke verarbeitet werden“. Schon damals stellten sie fest, dass „das direkte Einbinden von Social Plugins, beispielsweise von Facebook, Google+ oder Twitter, in Websites deutscher Anbieter, wodurch eine Datenübertragung an den jeweiligen Anbieter des Social Plugins ausgelöst wird, [...] ohne hinreichende Information der Internetnutzerinnen und -nutzer und ohne ihnen die Möglichkeit zu geben, die Datenübertragung zu unterbinden“ unzulässig sei.

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)[11]

Auf der Webseite des BfDI findet sich unter dem Thema „Telefon und Internet“ der Beitrag „Facebook, Twitter und Co.: Datenschutz in Sozialen Netzwerken“. Auch wenn der BfDI hier nicht die Datenschutzaufsicht hat, stellt der Beitrag doch recht anschaulich die Gefahren heraus, die bei Veröffentlichungen in Sozialen Netzwerken drohen. Die Empfehlung dort lautet: „Aus datenschutzrechtlicher Sicht sollte man die Vor- und Nachteile der Preisgabe von persönlichen Informationen genau abwägen und die Persönlichkeitsrechte Dritter respektieren.“ Hier wird kurzerhand aus einem „Muss“ ein „Sollte“. Der BfDI fordert auch auf, jeweils die Datenschutzerklärung zu lesen, „denn diese konkretisiert die Erhebung und Verwendung der personenbezogenen Daten“. Ob dem so ist, muss stark bezweifelt werden, zeigen doch gerade die obigen Ausführungen, dass dies zumindest bei Twitter nicht der Fall ist. Positiv ist zu vermerken, dass erläutert wird, wer für die Datenschutzaufsicht zuständig ist. Allerdings wird dann lediglich auf die Impressumsseite des Netzwerkbetreibers verwiesen, der das Bundesland und damit die Aufsichtsbehörde entnommen werden soll. Am Beispiel Facebook wird dann die Datenschutzaufsicht Irlands erwähnt. Hier würde sich sicher eine Übersicht zumindest über die Betreiber der größten sozialen Netzwerke empfehlen! Ob sich allerdings an diesem Punkt etwas mit der kürzlich erfolgten Neubesetzung des Amtes durch Ulrich Kelber ändert, ist fraglich, da dieser bisher sehr intensiv seinen Twitter-Account bestückt (als MdB 19.000 Follower und 28.000 Tweets).

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Nun richtet sich das BSI natürlich in erster Linie an Behörden und Unternehmen und zählt in seiner Veröffentlichung „Soziale Medien und Soziale Netzwerke“[12] die Risiken auf: „Bei der rein privaten Nutzung von sozialen Medien sind maßgeblich die folgenden Sicherheitsrisiken als kritisch zu bewerten: Identitätsdiebstahl, Offenlegung privater Informationen / Schutz der Privatsphäre, Datenschutzverletzung, Phishing, Mobbing und Cyberstalking.“ In der Broschüre wird weiter herausgestellt, dass sich die Nutzung sozialer Medien für Unternehmen anders darstellt als die Privatnutzung, und sie legt den Schwerpunkt auf die Betrachtung des Abflusses von geschäftskritischen Informationen. Dieser kann nicht nur durch bewusste Informationsweitergabe geschehen, sondern das BSI führt auf, dass über Kontakte interne und externe Strukturen sichtbar werden. Fotos enthalten Informationen nicht nur im Bild, sondern auch in den Metadaten (z. B. Ortsangaben und Datumsstempel). Zu den dann dargestellten Strategien gehört schließlich auch die Empfehlung an das Unternehmen, eine eindeutige Regelung bezüglich der zu veröffentlichenden Informationen zu treffen: „Geschäftszahlen, Personalien oder strategische Informationen sollten explizit ausgeschlossen werden. Gleiches gilt für Kundenbeziehungen und Produktinformationen, die nicht auch auf dem offiziellen Internetauftritt des Unternehmens frei zugänglich sind“.

Unter Datenschutzgesichtspunkten gibt das BSI Unternehmen und Behörden die Empfehlung, „zumindest die wichtigen Teile der öffentlichen Internetpräsenz nicht exklusiv in sozialen Medien geschehen zu lassen“ und die Erläuterung, warum für Tweet-Buttons zumindest eine Zwei-Klick-Lösung vorzusehen ist. Sowohl hinsichtlich der privaten als auch der dienstlichen Nutzung durch Unternehmensangehörige macht es Vorschläge für Policies, die als Leitfäden zu verstehen und entsprechend anzupassen sind.

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg[13]

Die weitestgehende Aktivität in Richtung Twitter hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württembergs, Stefan Brink, entwickelt. Er führte eine Datenschutzfolgenabschätzung nach der Europäischen Datenschutzgrundverordnung (DSGVO) durch. Darin betont er seine Mitverantwortung, erklärt aber, dies bedeute nicht, „dass der LfDI die Datenschutzkonformität der Produkte der Twitter Inc. bestätigt oder garantiert". Doch will er „zukünftig auf die Anbieter einwirken, ihre Angebote transparenter und datenschutzfreundlicher zu gestalten". Zudem ist er überzeugt, dass mit seinem Twitter-Account „eine große Gruppe von Nutzern erreicht, begleitet und beraten wird, die auf anderen Wegen, z. B. über die Homepage oder mithilfe von Broschüren etc., nicht erreichbar ist".

Zwar ist ihm bewusst, dass seine Twitternutzung „die Menge der Daten, die von der Twitter Inc. verwendet und ausgewertet werden", erhöht, in der Risikoanalyse kommt er allerdings zum Schluss, dass die Schäden durch den LfDI-Account nur unwesentlich vergrößert werden. An dieser Stelle kann hinterfragt werden, wie groß die Gruppe wirklich ist, die der LfDI in Baden-Württemberg über sein Twitter-Angebot erreicht. Schließlich nutzte 2017 laut ARD/ZDF-Onlinestudie[14] nur 1 % der Gesamtbevölkerung Twitter täglich und 3 % wöchentlich. 2018 ist nur die wöchentliche Nutzung auf 4 % gestiegen. Der Twitter-Account des LfDI hat derzeit knapp 3.000 Follower. Überzeugen kann deshalb lediglich das Alternativangebot, die Tweets auch auf der LfDI-Homepage lesen zu können.

Abschließend kommt die Datenschutzfolgeabschätzung zu folgendem Ergebnis: „Die Twitternutzung durch den LfDI ist angesichts der beschriebenen Risiken und verbindlich vorgesehenen Maßnahmen vertretbar. Der LfDI verpflichtet sich, die weitere Entwicklung zu beobachten und die hier vorgenommene Prüfung regelmäßig, mindestens einmal im Quartal, zu wiederholen und ggfls. fortzuentwickeln." Also bleibt abzuwarten, wie diese regelmäßige Überprüfung und die Fortentwicklung aussieht. Auf Twitter wird sicher darüber berichtet.

Resümee

Anhand der Übersicht über die Grundfunktion von Twitter und die Ausschnitte aus der Twitter-Datenschutzrichtline konnte aufgezeigt werden, dass Twitter beliebige Datenauswertungen zu eigenen Gunsten vornimmt. Darüber hinaus wurde dargestellt, welche Auswertungen Dritte vornehmen können. Weitere Konsequenzen der Nutzung des öffentlichen Datenpools konnten nur angedeutet werden. Der Überblick über Stellungnahmen einschlägiger Behörden zeigt deren generelle Hilflosigkeit im Umgang mit dem global agierenden Social-Media-Konzern. Selbst der baden-württembergische LfDI fordert in seiner Richtlinie zur Nutzung Sozialer Medien durch öffentliche Stellen[15] angesichts „offensichtlicher datenschutzrechtlicher Defizite bei einer Reihe Sozialer Netzwerke" lediglich „Datensparsamkeit", „Aufklärung" und „einen Hinweis auf die eigenverantwortliche Nutzung".

Aber warum nutzen öffentliche Stellen und speziell Datenschutzbeauftragte überhaupt Twitter? Eine Analyse von Zahlen und Effekten in einer wirklich kritischen Datenschutzfolgenabschätzung steht noch aus. Über Alternativen zu Twitter soll zu einem späteren Zeitpunkt berichtet werden.

1 https://cdn.cms-twdigitalassets.com/content/dam/legal-twitter/site-assets/privacy-page-gdpr/pdfs/PP_Q22018_April_DE.pdf

2 Social Media und Microtargeting in Deutschland. Informatik Spektrum: Vol. 40, No. 4. Berlin Heidelberg: Springer-Verlag, (S. 327-335).

3 https://www.uni-marburg.de/de/aktuelles/news/islamwissenschaftler-erforschen-tuerkischen-atheismus und https://www.giessener-anzeiger.de/amp/lokales/stadt-giessen/nachrichten-giessen/hegemonie-und-widerstand-in-der-turkei_18520125

4 https://www.derstandard.de/story/2000085466653/maschinelle-intelligenz-fuer-den-katastrophenfall

5 Pfaffenberger, F. (2016). Twitter als Basis wissenschaftlicher Studien: Eine Bewertung gängiger Erhebungs-und Analysemethoden der Twitter-Forschung. Springer-Verlag.

6 Nutzung soz. Medien durch stationäre Psychotherapiepatienten; O.M. Czech, K. Podoll, F. Schneider in Der Nervenarzt 9/2018. (S. 1050).

7 Mahmud, Jalal, Jeffrey Nichols, and Clemens Drews. „Home location identification of twitter users." ACM Transactions on Intelligent Systems and Technology (TIST) 5.3 (2014): 47.

8 Mahmud, Jalal, et al. „Predicting attitude and actions of twitter users." Proceedings of the 21st International Conference on Intelligent User Interfaces. ACM, 2016.

9 Arnoux, Pierre-Hadrien, et al. „25 Tweets to Know You: A New Model to Predict Personality with Social Media." arXiv preprint arXiv:1704.05513 (2017).

10 Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 08. Dezember 2011) https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/08122011DSInSozialenNetzwerken.pdf

11 https://www.bfdi.bund.de/DE/Datenschutz/Themen/Telefon_Internet/InternetArtikel/DatenschutzInSozialenNetzwerken.html

12 https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/SozialeNetze/Sicherheitsrisiken/sicherheitsrisiken_node.html

13 https://www.baden-wuerttemberg.datenschutz.de/twitter-datenschutzfolgenabschaetzung/

14 http://www.ard-zdf-onlinestudie.de/whatsapponlinecommunities/

15 https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2017/11/2017.11.02._Richtlinie-zur-Nutzung-sozialer-Netzwerke-durch-öff.-Stellen.pdf



Frans Valenta

Messenger – Eine kleine Orientierungshilfe

Jedes Mal, wenn ich neue Bekanntschaften mache, werde ich nach meiner Handynummer gefragt und gebeten, mich einer WhatsApp-Gruppe anzuschließen. Mein Einwand, dass WhatsApp alles andere als datenschutzfreundlich ist, und ich lieber per E-Mail oder SMS kommuniziere, wird meistens mit einem Kopfschütteln und dem Hinweis abgewehrt, dass bei WhatsApp doch alles kostenlos ist – selbst das Telefonieren oder der Videochat. Und überhaupt würden doch fast alle Menschen WhatsApp nutzen... So ist das also: „kostenlos“ und „weit verbreitet“ schlägt „Datenschutz“.



WhatsApp

Ich habe mir daraufhin Gedanken gemacht, wie WhatsApp genutzt werden kann, ohne die eigene wahre Identität preiszugeben. Für die Umsetzung werden zwei Smartphones benötigt. In dem ersten Smartphone muss keine SIM-Karte enthalten sein und es darf darauf keine Kontakt-Datei existieren. Das zweite Smartphone mit Prepaid-Karte ermöglicht die Bereitstellung einer Telefonnummer. Diese Telefonnummer, die möglichst noch niemand kennen sollte, dient zur eindeutigen Identifikation bei der Registrierung.[1] Nachdem WhatsApp auf dem Smartphone Nr. 1 heruntergeladen und installiert worden ist, möchte das Programm nach dem ersten Start die Erlaubnis des Zugriffs auf Kontakte, Fotos, Medien und Dateien auf dem Gerät. Immerhin gibt es die Auswahloption „Jetzt nicht“. Dann folgt im nächsten Schritt die Verifikation mit der Eingabe der Telefonnummer von Smartphone 2. Im Prinzip würde es auch mit einer Festnetznummer funktionieren, sofern eine SMS empfangen werden kann. Nach dem Absenden der Telefonnummer auf Smartphone 1 schickt WhatsApp eine SMS mit einem sechsstelligen Freischaltcode auf Smartphone 2. Mit der Eingabe dieses Codes auf Smartphone 1 ist nach Eingabe eines realistisch klingenden Phantasienamens das Gerät freigeschaltet und zeigt den Status-Datenschutz, der auf „Nur teilen mit...“ eingestellt werden sollte. Unter dem Menüpunkt „Chats“ fordert WhatsApp dazu auf, Freunde einzuladen. Mit dem runden Button unten rechts geht es weiter und hier lässt sich über „Neuer Kontakt“ eine (zunächst anonyme) Verbindung zu Personen und Gruppen herstellen. Ganz anonym zu bleiben ist auf Android- und iPhone-Smartphones wegen der Existenz der Werbe-ID[2] und Device-ID[3] etwas problematisch. Diese Kennnummern werden vom Hersteller des jeweiligen Betriebssystems zugeteilt, also von Google oder Apple. Da WhatsApp Geld mit Werbung verdient, ist das Interesse an effektiver und personalisierter Werbung groß. Deswegen möchte WhatsApp seine Nutzer möglichst eindeutig identifizieren können. Mit Hilfe der bereitgestellten IDs gelingt das in den meisten Fällen. Aber zumindest die Werbe-IDs lassen sich zurücksetzen und alle Apps vergessen schlagartig die Vorlieben.[4]

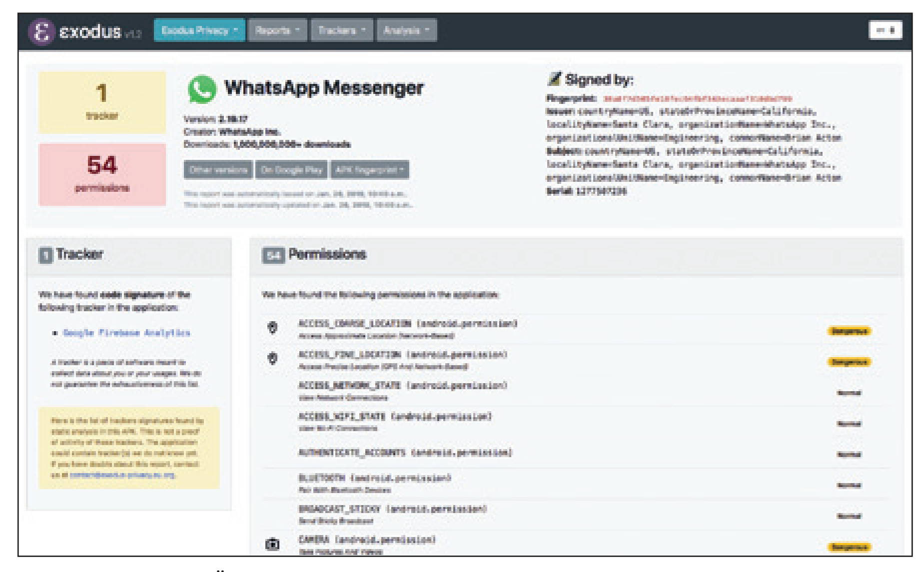
Wer wissen möchte, was WhatsApp an Berechtigungen einfordert, sollte sich das Programm „Exodus“ anschauen. Die Software von Meteo France ist für Android als App verfügbar und Anfragen zu den Berechtigungen von verschiedenen Apps können auch über den Browser auf dem Desktop durchgeführt werden. Exodus listet 54 Berechtigungen auf, von denen 12 als gefährlich eingestuft werden.[5]

Aber was bedeutet schon „Gefahr“, wenn es doch so schön bequem ist? WhatsApp hat eine große Fangemeinde und diese betrachtet „ihr“ Programm als alternativlos. Dabei gibt es nicht nur seit den Enthüllungen von Edward Snowden eine sehr große Zahl von Messenger, die ein höheres Maß an Sicherheit und Privatsphäre bieten.



Telegram

Mir wurde oft „Telegram“ als Alternative empfohlen. Telegram – ursprünglich in Russland entwickelt – hat sich nach der Übernahme von WhatsApp durch Facebook und den damit verbundenen Datenschutzbedenken der Nutzergemeinde als kostenlose Alternative etablieren können. Inzwischen gibt es nach



Ein Ausschnitt aus der Übersicht von exodus-privacy.eu.org

Firmenangaben 150-200 Millionen Nutzer.[6] Auf der Webseite befindet sich kein Impressum, aber im F.A.Q.-Bereich gibt es den Hinweis, dass die Entwicklung in Dubai stattfindet.[7] Der Dienst wirbt mit Sicherheit und Transparenz, aber bei dem Versuch, genaue Fakten zusammenzutragen, zeigt sich, dass hinter Telegram ein undurchsichtiges Netz aus zum Teil in Steueroasen niedergelassenen Briefkastenfirmen existiert.[8]

Telegram wird zwar als sicher beworben, dennoch gelang es dem Bundeskriminalamt den Messenger zu hacken.[9] Die Ende-zu-Ende-Verschlüsselung des Messengers ist nämlich nur aktiv, wenn man sie manuell einschaltet. Die Einstellungen sind jedoch nicht leicht zu finden. Für Gruppenchats funktioniert die Verschlüsselung gar nicht.

Bei einer Veranstaltung mit 1500 Studenten und 7500 Online-Zuschauern in Innsbruck am 18. Oktober 2018 äußerte sich der live zugeschaltete Edward Snowden: „Benutzt Signal, statt Telegram oder die Facebook Messenger, verschlüsselt eure E-Mails, benutzt offene Software statt Windows. Das rettet Euch nicht, macht Euch aber zu einem schwerer zu treffendem Ziel“. [10]



Signal

Die empfohlene Alternative Signal[11], die für alle gängigen Betriebssysteme verfügbar ist, wird von Open Whisper Systems entwickelt, die unter Anderem von dem ehemaligen WhatsApp-Mitbegründer Brian Acton[12] über die Signal-Stiftung[13] mitfinanziert wird. Sie erfordert wie WhatsApp zur Benutzung zwingend eine Telefonnummer. Um trotzdem Anonymität zu gewährleisten, wird von Signal statt der Telefonnummer der anonyme mathematische Fingerabdruck an den Server zum Abgleich geschickt. Es ist das Ziel der Betreiber, selbst keine Kenntnis davon zu haben, wer mit wem wann worüber kommuniziert. Der Quellcode ist öffentlich über GitHub verfügbar. Die Ende-zu-Ende-Verschlüsselung gilt als sehr sicher[14] und wurde 2014 auch von WhatsApp übernommen. Eine Kommunikation zwischen WhatsApp und Signal ist jedoch nicht möglich. Bei der Installation wird ein Zugriff auf das Adressbuch verlangt, um andere Nutzer zu finden. Wird der Zugriff verweigert, muss die Telefonnummer des Empfängers per Hand eingetippt werden und sie kann nicht in der Kontaktliste gespeicht werden. Die Macher von Signal geben an, dass Kontaktdaten grundsätzlich anonymisiert (gehasht) auf Signals Servern abgeglichen und anschließend wieder gelöscht werden.

Signal kann verschlüsselte Textnachrichten, Dokumente, Fotos, Videos, Kontaktinformation eins zu eins oder in Gruppennachrichten übertragen. Die Nachrichten werden über die in den USA befindlichen Server von Open Whisper Systems geleitet. Durch die Verschlüsselung können die Inhalte jedoch vom Betreiber nicht gelesen werden und sind auch vor Behörden sicher. Leider setzen die Desktop-Versionen wegen des Telefonnummern-Zwangs ein Smartphone voraus, mit dem sie beim ersten Start per QR-Code gekoppelt werden.



Threema

Eine weitere Messenger-Option ist Threema.[15] Die kostenpflichtige App aus der Schweiz ist nur für Smartphones und Tablets verfügbar. Der Bezeichnung Threema ist das Akronym EEEMA, die Abkürzung für End-to-End-Encrypting Messaging Application, vorausgegangen, wobei die drei E durch den Begriff Three (Englisch für drei) ersetzt wurden.[16]

Wie bei Telegram führte 2014 die Übernahme von WhatsApp durch Facebook sprunghaft zu einer Zunahme der Nutzerzahlen, die im Januar 2018 nach Angaben des Unternehmens bei 4,5 Millionen lag.

Beim ersten Start erstellt Threema zur Identifizierung ihrer Nutzer eine ID. Die App benötigt weder eine Telefonnummer noch den Zugriff auf das Adressbuch. Sicherheitsaspekte stehen im Vordergrund und daher werden keine Metadaten erhoben und Kontakte nur anonymisiert abgeglichen. Eine Ende-zu-Ende-Verschlüsselung für Chats, Gruppen-Chats und Audio-Telefonie steht standardmäßig zur Verfügung. Bei einem Sicherheits-Audit haben Prüfer der IT-Firma Cnlab Security AG festgestellt, dass die Verschlüsselung keine Schwächen aufweist.[17] Zur Sicherheit trägt auch die Tatsache bei, dass Threema seine Server in der Schweiz betreibt. Allerdings ist der Quellcode nicht frei zugänglich.

wire

Wer eine sichere Software sucht, die auf Open Source basiert, nicht zwingend eine Telefonnummer benötigt und für fast alle Betriebssysteme auf Mobilgeräten und Desktop verfügbar ist, wird bei Wire[18] fündig. Wire gibt es in Ausführungen für den kostenlosen privaten Gebrauch und kostenpflichtige Nutzung für Unternehmen. Die Betreiberfirma Wire Swiss GmbH sitzt in der Schweiz. Die softwaretechnische Weiterentwicklung des Messengers findet in Berlin statt. Nach Angaben des Unternehmens werden in der EU befindliche Server von Amazon verwendet. Das Entwicklungsteam besteht aus ehemaligen Mitarbeitern von Apple, Skype, Nokia und Microsoft.

Bei der Registrierung müssen ein Name, ein Benutzername und eine E-Mail-Adresse oder eine Telefonnummer angegeben werden.[19] Optionale Adressbuch-Daten liegen nicht auf den Wire-Servern, sondern werden nur flüchtig zwischengespeichert[20]. Aus den Adressbüchern werden keine weiteren Informationen wie Namen, Adressen, Geburtsdaten, Notizen usw. extrahiert.

Zur Verschlüsselung macht Wire auf der Webseite folgende Angaben:

„Textnachrichten und Bilder werden mit dem Proteus Protokoll Ende-zu-Ende verschlüsselt. Proteus basiert auf dem Axolotl-Ratchet und Pre-Keys, die für mobiles und Multi-Device-Messaging optimiert wurden. Sprach- und Videoanrufe verwenden den WebRTC-Standard. Wires Verschlüsselung arbeitet transparent im Hintergrund und muss nicht erst eingeschaltet werden – sie ist stets aktiviert.“

Die Verbreitung von Wire ist derzeit noch gering, obwohl die Software in Messenger-Vergleichslisten im Internet gute Beurteilungen bekommt, zum Beispiel bei Wikipedia[21] oder bei securemessagingapps.[22]

Freunde und Bekannte bei der Online-Kommunikation von Datenschutz und Sicherheit zu überzeugen ist mühsam, aber die notwendige Aufklärung trägt dazu bei, eine höhere Sensibilisierung bezüglich der Datensammelwut beliebter Messenger zu erzeugen und die Installation eines zusätzlichen sichereren Messengers anzustoßen.

1 https://faq.whatsapp.com/de/android/20970873/ und https://faq.whatsapp.com/de/iphone/20902747/?category=5245245

2 https://mobilsicher.de/hintergrund/smartphone-nutzer-sollten-jetzt-ihre-werbe-id-aendern

3 https://mobilsicher.de/hintergrund/was-sind-identifier-android und https://support.apple.com/de-de/HT204073

4 https://www.checked4you.de/handy-telefon/apps/app-und-ad-tracking-für-android-und-ios-deaktivieren-351073

5 https://reports.exodus-privacy.eu.org/en/reports/57651/

6 https://www.netzpiloten.de/telegram-messaging-app-vertrauen/

7 https://telegram.org/faq#q-what-is-telegram-what-do-i-do-here

8 https://www.gruenderszene.de/allgemein/telegram-berlin-oder-nicht

9 https://mobilsicher.de/kategorie/whatsapp-und-messenger/messenger-telegram-ist-unsicher

10 https://www.t-online.de/digital/id_84641084/edward-snowden-warnt-vor-facebook-messenger-und-telegram.html

11 https://signal.org

12 https://www.heise.de/newsticker/meldung/Krypto-Messenger-WhatsApp-Mitgruender-investiert-50-Millionen-Dollar-in-Signal-Stiftung-3975878.html

13 https://en.wikipedia.org/wiki/Signal_Foundation

14 https://eprint.iacr.org/2016/1013.pdf

15 https://threema.ch/de

16 https://de.wikipedia.org/wiki/Threema

17 https://www.heise.de/security/meldung/Threema-Audit-abgeschlossen-Ende-zu-Ende-Verschluesselung-ohne-Schwaechen-2868866.html

18 https://wire.com/de/

19 https://wire-docs.wire.com/download/Wire+Privacy+Whitepaper.pdf

20 https://www.datenschutzbeauftragter-info.de/wire-sichere-skype-und-whatsapp-alternative/

21 https://de.wikipedia.org/wiki/Liste_von_mobilen_Instant-Messengern

22 https://www.securemessagingapps.com

Gemeinsame Pressemitteilung zum ePrivacy-Gespräch beim Bundesministerium für Justiz und Verbraucherschutz vom 22.01.2019

ePrivacy: EU-Regierungen wollen elektronische Nachrichtenzensur einführen

Die Bundesregierung tritt nach eigenen Aussagen in den Verhandlungen zur ePrivacy-Verordnung für Verbesserungen des letzten Vorschlags der österreichischen Ratspräsidentschaft ein, wie die Begrenzung der zweckfremden Nutzung von Kommunikationsdaten oder datenschutzfreundliche Voreinstellungen in Browsern.

Einige EU-Regierungen wollen nun aber mit der Einführung der ePrivacy-Verordnung Internetverbindungen, E-Mails und Whatsapp-Nachrichten auf unzulässige Inhalte durchsuchen lassen. Zum Auffinden von „kinderpornografischen“ und „terroristischen“ Inhalten sollen Internetprovider, E-Mail-Anbieter und Anbieter von Messaging-Diensten nach eigenem Ermessen die Internetnutzung und versandte Nachrichten ihrer Kunden verdachtslos und flächendeckend filtern dürfen. Das in der geplanten ePrivacy-Verordnung vorgesehene Telekommunikationsgeheimnis soll insoweit aufgehoben werden. Durch nationale Gesetze könnte die Nachrichtenzensur zudem verpflichtend eingeführt werden.

In einem Gespräch auf Einladung des Bundesjustizministeriums am 21.01.2019 in Berlin kritisierten Bürgerrechts- und Datenschutzorganisationen einen solchen Versuch der Prinzipienumkehr scharf. Mit Blick auf übliche Verschlüsselungstechnologie wurden die insbesondere von Großbritannien vorangetriebenen Zensurpläne, mit denen sich am Donnerstag eine Ratsarbeitsgruppe befassen soll, als wirkungslos bezeichnet.

Auch die Ratspläne zur ausufernden Sammlung und Weitergabe von Positions- und Verbindungsdaten durch Telekommunikationsanbieter sowie zur Zulassung einer Durchleuchtung des Surfverhaltens für Werbezwecke (Tracking) werden kritisch gesehen. Stattdessen forderten die Vertreter der Zivilgesellschaft ein Recht auf datenschutzfreundliche Browsereinstellungen, einen besseren Schutz vor Datenklau und Abhören sowie einen zügigen Abschluss der verschleppten ePrivacy-Reform.

Das federführende Wirtschaftsministerium stellte ein baldiges Nachfolgegespräch in Aussicht. Es wurde zuletzt öffentlich vielfach kritisiert, dass bisher fast nur mit Wirtschaftsverbänden über die ePrivacy-Reform gesprochen wurde. Begrüßt wird auch, dass geprüft wird, ob die im Rat eingebrachten Formulierungsvorschläge der Bundesregierung veröffentlicht werden.

Der Wille scheint in der Regierung weiterhin groß zu sein, die ePrivacy-

Verordnung zu einem Abschluss zu bringen. Aus Sicht der Verbände ist das überfällig. Dabei ist auf eine bessere Berücksichtigung digitaler Bürgerrechte, wie vom Europäischen Parlament gefordert, zu hoffen.

An dem Gespräch teilgenommen hatten Vertreter von Arbeitskreis Vorratsdatenspeicherung, Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V., Deutsche Vereinigung für Datenschutz (DVD) e.V., die Datenschützer Rhein Main, Digitalcourage, Digitale Gesellschaft, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V., ISOC.DE, Netzwerk Datenschutzexpertise.

Roland Appel

War es das, Frau Voßhoff?

Vier Jahre lang hat die Bundesbeauftragte für den Datenschutz nichts Nennenswertes gesagt. Sie hat zu neuen Fahndungsinstrumenten wie der Gesichtserkennung in der Videotechnik geschwiegen, hat zu den Skandalen von Google, Facebook und Cambridge Analytica kein Wort gesagt. Sie hat erst kürzlich einen der übelsten Gesetzentwürfe des Bundesverkehrsministers durchgewunken, der sämtliche Kennzeichen von Fahrzeugen erfassen und verdachtsunabhängig abgleichen soll, obwohl es ein eindeutig einfacheres und mit keinen derart gravierenden Grundrechtseingriffen verbundenes Mittel gäbe: die blaue Plakette für umweltfreundliche Fahrzeuge. Sie war auf internationalen Konferenzen der Datenschützer nicht vorhanden und hat – anstatt Bürger und Wirtschaft über die Datenschutz-Grundverordnung aufzuklären – sich einen Tag vorher belanglos dazu geäußert und dann wieder zum Büroschlaf in ihr Bonner Büro zurückgezogen.

Eine größere Versagerin im Amt hat die Bundesrepublik in keinem öffentlichen Amt in den letzten vierzig Jahren ertragen müssen. Eigentlich müsste sie wegen Arbeitsverweigerung verklagt und ihr die Ruhestandbezüge wegen Untätigkeit entzogen werden. Und nun, wenige Tage vor Ende ihrer Amtszeit, gab sie ein Interview, in dem sie die Automobilkonzerne dafür verantwortlich macht, dass China mit der Elektromobilität einen Überwachungsstaat etabliert, der seinesgleichen sucht. Es trifft alles zu, was sie im Interview mit Heise kritisiert (https://heise.de/-4258216). Es ist auch seit mindestens drei Jahren bekannt und von den Automobilkonzernen und deren Datenschutzbeauftragten immer wieder an die Datenschutzbeauftragte herangetragen worden. Auf dem letzten Nachhaltigkeitsdialog eines Stuttgarter Herstellers im November 2018 erst war der chinesische Überwachungsstaat Thema, NGO und kritische Sachverständige trugen ihre Besorgnis über das Social Credit System Chinas auf Einladung des Vorstands vor. All dieses ist der Datenschutzbeauftragten seit langem bekannt – ebenso wie der Marktmechanismus und die Rechtslage, die jedem Unternehmen keine andere Entscheidungsmöglicheit gibt, als sich an chinesische Gesetze zu halten.

Anstatt folgenloses Konzernbashing zu betreiben, hätte Frau Voßhoff in der Sache hilfreich sein können, indem sie bei der Bundesregierung genau in dieser Frage interveniert hätte. Sie hätte dafür sorgen können, dass die Kanzlerin diese Überwachungsprobleme beim pompösen Staatsbesuch des chinesischen Parteichefs Xi anspricht, in den Korb der Menschenrechte aufnimmt. Denn nur, wenn an anderer Stelle Sanktionen drohen – z. B. bei der Frage der Investition oder dem Kauf deutscher Unternehmen – können Menschenrechtsverletzer wie Xi überzeugt werden, dass nicht alles gemacht werden darf, was sie gerne möchten.

Aber auch hier war Frau Voßhoff ebensowenig präsent wie auf den IT-Gipfeln der Bundesregierung, zu dem sie sich auch einmal hätte kritisch äußern können – schließlich wollen nach wie vor Bundesregierung und IT-Wirtschaft die persönlichen Daten der Bürgerinnen und Bürger zur Beute machen, fabulieren vom „Datenschatz heben“ = in die Privatsphäre des Einzelnen einbrechen. Dann kündigt die Bundesregierung gleich mal eine zentrale Patientendatenhaltung für alle Bundesbürger an. Zu „Smart Cities“, mit Überwachung an jeder Straßenlaterne und jeder E-Ladestation, „Smart Homes“ mit „Alexas“ Aufzeichnung intimster Dialoge in Wohn- und Schlafzimmern, „Smart Kühlschränken“ mit Überwachung unseres täglichen Konsums hätte sie vielleicht einmal das eine oder andere bewertende Wort verlieren können. Ihre Vorgänger, ob mit grünem, FDP-, SPD- und sogar CSU-Parteibuch haben davon in der Vergangenheit reichlich Gebrauch gemacht.

Nicht Frau Voßhoff. Sie hat den Gegenwert für ihren Mandatsverlust im Bundestag einfach still abgesessen. Fünf Jahre hatte sie bekommen. Viereinhalb Jahre Schweigen – und nun eine theatralische Geste des Alarmismus gegenüber Datenmissbrauch in einem Land, wo die Überwachung ohnehin System hat? Aber vielleicht dachte sie ja, wenn sie schweigt, kommt sie wegen guter Führung früher frei und in Rente.

Si tacuisses – Ach, wenn sie doch geschwiegen hätte! (leicht überarbeitete Fassung eines Beitrags des Autors im Beueler Extradienst vom 28.12.2018, www.extradienst.net).

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Ulrich Kelber wird neuer BfDI

Der frühere Justiz- und Verbraucherschutzstaatssekretär des Bundes Ulrich Kelber löst Andrea Voßhoff an der Spitze der Bundesdatenschutzbehörde ab. Mit der Mehrheit von 444 zu 176 Stimmen bei 37 Enthaltungen hat der Bundestag am 29.11.2018 den Diplom-Informatiker Ulrich Kelber zum neuen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) gewählt (vgl. DANA 2/2018, 102). Der SPD-Abgeordnete löst damit Anfang 2019 die CDU-Rechtspolitikerin Andrea Voßhoff an der Spitze der unabhängigen Behörde mit Sitz in Bonn ab. Diese Behörde soll die Einhaltung der datenschutzrechtlichen Vorschriften in der Bundesverwaltung sowie im Post- und Telekommunikationsbereich kontrollieren und über Risiken im Umgang mit personenbezogenen Daten aufklären. Kelber selbst bezeichnete als eine seiner wichtigsten Aufgaben im neuen Amt, das europaweite Datenschutzrecht durchzusetzen: „Die europaweite Harmonisierung beim Datenschutz ist Voraussetzung dafür, auch den großen, nichteuropäischen Internetkonzernen auf Augenhöhe begegnen und unsere europäischen Datenschutzstandards durchsetzen zu können."

Ein weiteres bedeutendes Thema sei, dass der Staat seine Dienstleistungen verstärkt auch auf digitalen Wegen anbieten werde, was aber nicht dazu genutzt werden dürfe, noch mehr Informationen über die BürgerInnen zu sammeln. Bei den Sicherheitsbehörden wolle er ein Auge darauf werfen, dass sie angesichts ihrer in den jüngsten Jahren massiv ausgebauten Befugnisse „vorbildlich die Grundprinzipien des Datenschutzes einhalten". Auf EU-Ebene komme es darauf an, „den Datenschutz weiterzuentwickeln und dabei Profiling und Scoring effektiv zu regulieren". Hierzulande müsse die Idee der Informationsfreiheit ausgebaut werden.

Kelber gilt im Gegensatz zu seiner Vorgängerin, die bei Amtsantritt keinerlei Datenschutzkenntnisse vorweisen konnte und sich während ihrer gesamten Dienstzeit mit öffentlichen Äußerungen zurückhielt (siehe den Beitrag von Appel, S. 27), bereits als Datenschutz- und Digitalexperte. Als parlamentarischer Staatssekretär machte er sich unter anderem für einen klareren Rechtsrahmen beim Scoring zur Bonitätsprüfung sowie einfachere Datenschutzerklärungen für Webseiten oder Apps in Form sogenannter One Pager stark.

Nach seinem Ausscheiden aus der Regierung kritisierte Kelber im März 2018 Digitalstaatsministerin Dorothee Bär (CSU) scharf für ihre Ansicht, dass in Deutschland „ein Datenschutz wie im 18. Jahrhundert" vorherrsche. Es gehe hier um den Grundrechtsschutz (DANA 2/2018, 103). 2011 hatte er sich gegen einen Beschluss der SPD für die verdachtsunabhängige monatelange Vorratsdatenspeicherung ausgesprochen. Vier Jahre später stimmte er aber im Parlament mit der großen Koalition dafür, eine solche verdachtsunabhängige Protokollierung von Nutzerspuren mit verkürzten Speicherfristen wieder einzuführen. Dagegen sind zahlreiche Beschwerden vor dem Bundesverfassungsgericht anhängig. Kelber übernimmt von Voßhoff eine im Vergleich zu den Landesdatenschutzbeauftragten gut ausgestattete Behörde. Mit Rückendeckung aus der CDU/CSU-Fraktion wurde die Zahl der Mitarbeitenden fast verdoppelt. Fraglich bleibt, ob dies genügt, um alle mit der Datenschutzgrundverordnung (DSGVO) verbundenen Herausforderungen zu meistern.

Wegen des praktizierten Auswahlverfahrens für den BfDI ernteten die Regierungsfraktionen Kritik. Jeweils im Wechsel darf eine an der Regierung beteiligte Fraktion einen Kandidaten benennen. Im Fall von Kelber waren die Sozialdemokraten an der Reihe. Malte Engeler, Richter am Schleswig-Holsteinischen Verwaltungsgericht, verwies darauf, dass nach Artikel 53 DSGVO die Spitze einer Datenschutzaufsichtsbehörde „im Wege eines transparenten Verfahrens ernannt" werden muss. Ein solches sei mit der bisherigen Praxis ohne öffentliche Stellenausschreibung samt entsprechender Auswahl- und Ernennungsvorgaben nicht gegeben. Der grüne Fraktionsvize Konstantin von Notz erklärte: „Das Verfahren ist das der großen Koalition. Wir hätten es uns auch gut anders vorstellen können. Den vorgeschlagenen Kandidaten finden wir aber gut und halten ihn für fachlich geeignet." Die SPD-Netzpolitikerin Saskia Esken betonte, dass der Bundestag die Wahl in öffentlicher Sitzung vornehme. Dies stelle „ein Höchstmaß an demokratischer Legitimation und Transparenz dar". Wer solche Spitzenämter besetzen solle, verabredeten die Parteien und Fraktionen klar im Rahmen der Koalitionsverhandlungen. Generell halte sie Kelber für einen „hochkompetenten und hochengagierten, überzeugten Datenschützer", mit dessen Einsatz ein hohes Durchsetzungsniveau mit „den Chancen der Datennutzung für sozialen, wissenschaftlichen und wirtschaftlichen Fortschritt" versöhnt werden könnten (Krempl, Ulrich Kelber: Bundestag wählt Informatiker zum Bundesdatenschutzbeauftragten, www.heise.de 29.11.2018; Kurzlink: https://heise.de/-4235690; zum Bestellungsprozess siehe auch die Analyse und den Überblick bei https://www.netzwerk-datenschutzexpertise.de/dokument/bestellung-oeffentlicher-datenschutzbeauftragter).

Bund

Verstärkte Überwachung von Ausreisepflichtigen geplant

Das Bundesinnenministerium hat den Bundesländern Vorschläge für be-

schleunigte Abschiebungen abgelehnter Asylbewerbender unterbreitet. Die Maßnahmen sollten dazu dienen, die Menschen noch schneller und einfacher als bisher in das für das Asylverfahren zuständige EU-Land zu überstellen, wo sie ihr Asylverfahren betreiben könnten, so das Ministerium am 18.11.2018 in Berlin. Auch gesetzliche Anpassungen seien denkbar. In dem Fünf-Punkte-Plan schlägt das Ministerium „Maßnahmen zur Beschleunigung und Erleichterung des Dublin-Verfahrens" vor. Der Auftrag resultiere aus dem Beschluss des Koalitionsausschusses vom 05.07.2018.

Konkret geht es zum einen um eine nächtliche Meldepflicht für Ausreisepflichtige, wenn diese Gemeinschaftsunterkünfte verlassen. Bei Verstößen könne Haft angeordnet werden, „sofern die Umstände des Einzelfalls hierdurch Fluchtgefahr annehmen lassen". Weiter sollten Flüchtlinge in Aufnahme- und Rückführungszentren ihre Post nur noch mit einer Chipkarte abholen können. Bescheide sollten so tagesaktuell zugestellt werden können, ein Untertauchen solle entsprechend zügig festgestellt werden können. In Dresden gebe es schon ein solches System. Zudem sollten „No-name-Buchungen" bei Abschiebeflügen sicherstellen, dass Plätze an Bord nicht unbesetzt blieben, wenn ein Flüchtling vor seiner Abschiebung untertauche. In den Gemeinschaftsunterkünften sollten ferner Ärzte fest angestellt werden. Schließlich sei eine bundesweite Online-Überstellungsplattform geplant, auf die alle beteiligten Behörden Zugriff hätten.

Der Ministeriumssprecher betonte, „in Kürze" werde ein Gesetzentwurf vorgelegt, der Regelungen zu Ausreisepflichten und zur Durchsetzung von Abschiebungen enthalte. Die oben genannten Punkte seien aber nicht Gegenstand des Entwurfes mit dem Titel „Zweites Gesetz zur besseren Durchsetzung der Ausreisepflicht". In den ersten zehn Monaten des Jahren 2018 wurden gemäß Presseberichten 29.790 Wiedereinreisesperren gegen abgeschobene und kriminelle Flüchtlinge verhängt. Im Gesamtjahr 2017 seien es 39.160 Sperren gewesen (Innenministerium will Abschiebungen beschleunigen, www.aachener-nachrichten.de 18.11.2018).

Bundesweit

EU-Vertragsverletzungsverfahren droht wegen Schlechtausstattung der Aufsicht

In mehreren Bundesländern versinken die Datenschutzbehörden in Arbeit, die mit der Einführung der Datenschutz-Grundverordnung (DSGVO) am 25.05.2018 über sie hereingebrochen ist. Die Wahrscheinlichkeit, dass die Aufsichtsbehörden über Selbstanzeigen bei der EU mitteilen, dass sie wegen fehlender MitarbeiterInnen ihre Pflichten nicht erfüllen können, nimmt zu.

Entsprechende Signale kommen aus Sachsen, Mecklenburg-Vorpommern und Hamburg. Die vom Bund gegründete Stiftung Datenschutz erklärte, der hohe Beratungsbedarf für BürgerInnen und Unternehmen sei offenkundig, so Stiftungsvorstand Frederick Richter: „Die Unterausstattung der Datenschutz-Aufsichtsbehörden durch die meisten Länder ist ein Skandal." Württembergs Datenschutzbeauftragter Stefan Brink geht davon aus, dass es ein Vertragsverletzungsverfahren gegen Deutschland geben wird: „Die EU-Kommission ist bei Deutschland besonders sensibel und wird besonders schnell agieren, weil Deutschland beim Datenschutz Vorbild war." Der EU sei aus Gesprächen mit Datenschützern bereits bekannt, dass es in einigen Bundesländern Probleme gibt. Eine Sprecherin der Kommission teilte mit, es habe zahlreiche Gespräche und EU-Angebote zur Unterstützung der Behörden gegeben: „Die Kommission überwacht nun die Anwendung der Verordnung in allen Mitgliedstaaten."

Die Aufsichtsbehörde in Baden-Württemberg hat mit dem Wirksamwerden der DSGVO mit nunmehr 53,5 Planstellen 60% Zuwachs bekommen, so Brink: „Aber auch wir haben allergrößte Schwierigkeiten bekommen, in angemessener Zeit Fälle abzuschließen." Zu den neuen Aufgaben komme hinzu, dass mehr Fälle gemeldet werden, die schon nach altem Recht problematisch waren. „Die Menschen beschweren sich schneller."

In einigen Bundesländern haben die Behörden bereits vor der DSGVO ihren Aufgaben nur sehr eingeschränkt nachkommen können und seitdem keine oder kaum Verstärkung bekommen. Vor allem bei den Bundesländern im Osten und den Stadtstaaten ist das der Fall. Daran hat auch die DSGVO nichts geändert: Mecklenburg-Vorpommerns Datenschutzbehörde etwa hat nach wie vor 21 Mitarbeitende; nach Inkrafttreten der DSGVO wurden lediglich aus Aushilfsmitteln bezahlte Stellen in feste umgewandelt. Behördenleiter Heinz Müller hat deshalb einen Appell an die SPD-geführte Staatskanzlei geschickt: „Sie soll uns im Wege der Amtshilfe Personal zur Verfügung stellen. Uns fehlen Juristen, Techniker und Sachbearbeiter, und das wird nicht vorübergehen." Mit der Bitte um Abstellungen folgt Müller, früher parlamentarischer Geschäftsführer der SPD-Fraktion, einem Rat des Landesrechnungshofs. Der Landtag hatte zwar neun weitere Stellen bewilligt, aber sofort zur Überprüfung durch den Rechnungshof gesperrt. Müller kritisiert: „Dessen Gutachten ist das Papier nicht wert." Dort sei ihm auch geraten worden, andere Datenschutzbeauftragte um Amtshilfe zu bitten. „Das ist so intelligent wie der Ratschlag an einen Bettler, einen anderen Bettler um Kredit zu fragen."

Referatsleiter Andreas Schneider vom Sächsischen Datenschutzbeauftragten erklärte, seine Behörde könne mit der „personellen Ausstattung nicht in der Fläche wirklich wirksam werden." Zu 22 bestehenden Vollzeitstellen waren 15 Vollzeitstellen als zusätzlicher Bedarf ermittelt worden. Tatsächlich sei nun angestrebt, „dass wir mittelfristig vier Stellen erhalten." Schneider spricht von „Tausenden Meldungen, die noch zu bearbeiten sind". Eine weitere Digitalisierung des Meldeprozesses bei Datenschutzverstößen werde die Arbeit etwas vereinfachen, aber das grundsätzliche Problem zu knapper Ressourcen nicht lösen. Die Behörde teilt den BürgerInnen die Überlastung auch so offen mit. In einer Antwort mehr als zwei Monate nach der Anfrage heißt es: „Wegen der mit der (…) DSGVO einhergehenden Flut von Anfragen und Beschwerden (…) sowie des (…) enormen Aufgabenzuwachses in Verbindungen damit, dass personelle Verstärkungen meiner Behörde bislang immer noch ausstehen und mir

auch für die Zukunft nur in vollkommen unzureichendem Maße zugestanden worden sind, muss ich (...) mitteilten, dass es zu erheblichen zeitlichen Verzögerungen kommt."

Hamburg, wo Deutschlands derzeit sichtbarster Datenschutzbeauftragter Johannes Caspar tätig ist, berichtet von einer „seit einigen Jahren defizitären Ausstattungssituation". Sein Referent Martin Schemm ergänzt: „Wir laufen den quantitativen und qualitativen Veränderungen des Aufgabenbereichs der Aufsichtsbehörde hinterher." Die Folgen bekommen nicht nur die BürgerInnen zu spüren, so Mecklenburg-Vorpommerns oberster Datenschützer Müller: „Wir schaffen es auch nicht, Verwaltungsverfahren des Landes mit unserer Expertise zu begleiten. Es reicht gerade so für Stellungnahmen in Gesetzgebungsverfahren." Unangekündigte Prüfungen auf eigene Initiative hin seien kaum vorstellbar. Zudem sei es fast unmöglich, Veranstaltungen für Multiplikatoren anzubieten, obwohl es dazu den Wunsch aus der Wirtschaft gebe: „Es gibt viele Unternehmen, die die Regeln der DSGVO einhalten wollen, aber Hilfe brauchen, die wir gerne leisten würden."

Die schlechte Ausstattung ist auch ein Standortnachteil, heißt es aus Sachsen: „Wir sind nicht nur Aufsichtsbehörde, sondern auch Berater und Service-Dienstleister." Aus der Landespolitik verspüren die DatenschützerInnen neben Unverständnis auch Unwillen, für eine Aufgabe zu zahlen, die von der EU käme. Andere EU-Länder haben zum Teil andere Finanzierungsmodelle gefunden, so Brink: „Behörden finanzieren sich aus den Bußgeldern selbst und können hohe Bußgelder erzielen. Deutsche Datenschutzbeauftragte haben von Bußgeldverfahren nur den Aufwand, weil das Geld in den Landeshaushalt fließt." Das Modell aus dem Ausland kann auch zu Auswüchsen führen. In Portugal wurde ein Bußgeld von 400.000 Euro gegen ein Krankenhaus mit schlechtem Datenzugriffskonzept verhängt (DANA 4/2018, 210), was in Deutschland, so Brink, vielleicht zu einer Geldbuße von 20.000 Euro führen würde: „Mittelfristig werden die unterschiedlichen Maßstäbe auch zum Thema auf EU-Ebene werden. Es ist auch eine Frage ungleichen Wettbewerbs, wenn ein Automobilkonzern in Frankreich eine massive Millionenstrafe zahlen muss und in Deutschland für den gleichen Verstoß mit einer besseren Ermahnung davon kommt."

Noch will keine deutsche Datenschutzbehörde offiziell in Brüssel erklären, die Arbeit nicht zu schaffen. Aus Sachsens Datenschutzbehörde verlautet: „Eine Anzeige bei der EU wollen wir noch nicht anstrengen, sie wäre aber ultima ratio. Wir können nicht glauben, dass der Missstand von der Politik dauerhaft so vertreten wird und haben die Erwartung, dass wir mit unseren Argumenten überzeugen können." Mecklenburg-Vorpommern wartet auf Reaktion auf das Schreiben. Hamburgs Datenschützer verfolgen gespannt die Haushaltsberatungen. Von dort heißt es: „Die nächste Datenschutzkonferenz im Frühjahr ist der Zeitpunkt, die Situation zu analysieren und sich auf ein gemeinsames Vorgehen der Aufsichtsbehörden zu verständigen. Hier liegen dann alle Handlungsoptionen auf dem Tisch" (Wienand, Deutschland droht EU-Verfahren wegen Datenschutz, www.t-online.de 21.11.2018).

Bundesweit

Meldestelle für antisemitische Vorfälle gegründet

In Berlin hat sich nach dem Vorbild der Berliner Recherche- und Informationsstelle Antisemitismus (RIAS) ein Verein zur bundesweiten Koordinierung von Meldestellen judenfeindlicher Vorfälle gegründet. RIAS-Projektleiter Benjamin Steinitz erklärte: „Ziel des Bundesverbandes RIAS ist die Sicherstellung einer bundeseinheitlichen und zivilgesellschaftlichen Erfassung von antisemitischen Vorfällen." Man wolle mit dem neuen Meldesystem auch Vorkommnisse erfassen, die keinen Straftatbestand erfüllen und auch solche, die nicht mit direkter Gewalt verbunden sind. „Viele Juden zeigen antisemitische Straftaten nicht bei der Polizei an, weil sie resigniert haben." Zudem sei die Zuordnung von Delikt und Täter häufig zweifelhaft. Damit in der polizeilichen Kriminalstatistik (PKS) ein Vorfall als antisemitisch aufgeführt wird, müssen die zuständigen PolizeibeamtInnen bei der Feststellung der Tat diese als antisemitisch definieren. Die Polizeistatistiken würden blinde Stellen aufweisen.

Gemäß Steinitz wurden allein für Berlin 3.378 Vorfälle seit Anfang 2015 registriert, als mit der Arbeit begonnen wurde: „Oder anders ausgedrückt: Pro Tag sind es im Durchschnitt zwei bis drei Vorfälle. Deshalb wird von Berlin auch häufig als der Hauptstadt des Antisemitismus gesprochen." Aus anderen Teilen Deutschlands wurden im selben Zeitraum 797 Vorfälle registriert. Das Selbstverständnis von RIAS Berlin war es dabei immer, Ansprechpartner für Betroffene zu sein und sie dazu zu ermutigen, entsprechende Ereignisse zu melden. Auch will man ihnen die Schwellenangst vor den Ermittlungsbehörden nehmen. „Damit haben wir gute Erfahrungen gemacht und viel Vertrauen aufgebaut." Deshalb soll dieses System nun sukzessive auf ganz Deutschland ausgeweitet werden. Die Erfassung der Vorfälle soll sich an der Definition von Antisemitismus der Internationalen Allianz für Holocaustgedenken orientieren. Danach geht es um Worte oder Taten, die sich aus Hass gegen Juden speisen und sich auch gegen Personen und Institutionen richten können sowie gegen den Staat Israel.

Neben dem RIAS-Projektleiter gehören der Geschäftsführer des Zentralrats der Juden, Daniel Botmann, sowie die stellvertretende Geschäftsführerin des Vereins für Demokratische Kultur in Berlin (VDK), Anne Benzing, dem für zwei Jahre gewählten Vereinsvorstand des neuen Bundesverbandes RIAS an. Der Antisemitismusbeauftragte der Bundesregierung, Felix Klein, wird Schirmherr des Vereins.

Zur Gründung des bundesweiten Meldesystems am 31.10.2018 sagte Felix Klein: „Mit dem nun neu eingeführten bundesweiten, niedrigschwelligen Meldesystem für antisemitische Vorfälle möchten wir die Dunkelziffer verkleinern, die es derzeit noch gibt. Unser Anliegen ist es, die Realität von Antisemitismus in Deutschland für die gesamte Gesellschaft sichtbar zu machen und dadurch eine wichtige und empirisch belegte Grundlage für seine Bekämpfung zu schaffen." Das Bundesfamilienministerium beteiligt sich mit Mitteln

des Programms „Demokratie leben!“ an der Finanzierung der Meldestelle. In Brandenburg und Bayern haben sich bereits regionale Dokumentationsstellen für antisemitische Vorfälle gegründet. Auch die anderen Bundesländer sollen Kooperationspartner werden.

Zentralratsgeschäftsführer Daniel Botmann sagte, dass die Einführung einer bundesweiten Meldestelle ein wichtiger Schritt zur Bekämpfung von Antisemitismus sei: „Die offiziellen Statistiken spiegeln nicht die Wahrnehmungen innerhalb der jüdischen Community wider“. Für das Jahr 2017 zählte die PKS insgesamt 1.453 antisemitische Straftaten. Die Täter wurden zu 90% dem rechtsextremen Spektrum zugeordnet. RIAS kritisiert, dass diese Zahlen nicht das Ausmaß antisemitischer Vorfälle in Deutschland widerspiegeln und die Tätergruppen ungenau erfasst werden. Felix Klein ergänzte: „Aus den jüdischen Gemeinden höre ich, dass die subjektive Wahrnehmung der Bedrohung durch muslimisch geprägten Antisemitismus größer ist, als es in der Kriminalstatistik zum Ausdruck kommt.“ Deshalb müsse die Kriminalstatistik dringend überprüft, darüber hinaus aber auch ein niederschwelliges bundesweites Erfassungssystem antisemitischer Übergriffe eingeführt werden (Balke, Aus der Anonymität holen, www.juedische-allgemeine.de 20.12.2018; Lombard, Bundesweite Meldestelle für antisemitische Vorfälle gegründet, www.juedische-allgemeine.de 02.11.2018).

Mehrere Bundesländer

SID, BvD und Aufsichtsbehörden „gehen in die Schule“

Die Initiative „Datenschutz geht zur Schule“ vom Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. erhielt anlässlich des Safer Internet Day (SID) am 29.01.2019 dadurch Unterstützung, dass MitarbeiterInnen der Datenschutz-Aufsichtsbehörden von Baden-Württemberg, Bayern, Niedersachen und Rheinland-Pfalz im Folgemonat an den Schulen ihres jeweiligen Bundeslandes Unterrichtseinheiten für Kinder und Jugendliche zum sicheren Umgang mit persönlichen Daten im Internet anbieten. Gemäß dem Sprecher der BvD-Initiative, Rudi Kramer, hilft diese Kooperation, „viel mehr Heranwachsende beim Thema Datenschutz zu erreichen“. Sicher im Netz zu surfen sei eine Grundvoraussetzung für junge Menschen, selbstständig und bewusst eigene Entscheidungen online treffen zu können.

Stefan Brink, Landesbeauftragter für Datenschutz und Informationsfreiheit (LfDI) Baden-Württemberg, koordiniert auf Seiten der Aufsichtsbehörden das Projekt. Er wies drauf hin, dass allein in seiner Dienstelle sich mehr als zehn Mitarbeiterinnen und Mitarbeiter für die Unterrichtseinheiten gemeldet haben. Bei ihrem Unterricht greifen die Mitarbeitenden der Aufsichtsbehörden auf das BvD-Material von „Datenschutz geht zur Schule“ zurück, dessen Weiterentwicklung inhaltlich von der EU- Initiative klicksafe und finanziell von der DATEV-Stiftung Zukunft unterstützt wurde. Für Lehrkräfte, die selbst Aspekte des Datenschutzes im Unterricht behandeln oder die Einheiten vor- und nachbereiten wollen, liegt seit November 2018 die 3. neu überarbeitete Auflage des Lehrerhandbuchs „Datenschutz geht zur Schule“ vor. Die Materialien können kostenlos unter www.bvdnet.de/datenschutz-geht-zur-schule heruntergeladen werden. Die EU-Initiative klicksafe organisierte den Safer Internet Day am 05.02.2019 unter dem Motto „Together for a better internet“ und widmet sich im Schwerpunkt und unter dem Hashtag #lauteralshass gegen Hass im Netz. Seit 2004 findet der Safer Internet Day auf Initiative der Europäischen Kommission jährlich an dem zweiten Tag der zweiten Woche des zweiten Monats statt (LfDI Baden-Württemberg, BayLDA, Lfd Nds, LfDI Rheinland-Pfalz, Safer Internet Day, BvD e. V., PE 30.01.2019, „Datenschutz geht zur Schule“ startet in neue Ära).

Baden-Württemberg

Erstes DSGVO-Bußgeld

Wegen eines Verstoßes gegen die nach Art. 32 Datenschutz-Grundverordnung (DSGVO) vorgeschriebene Datensicherheit hat die Bußgeldstelle des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI) am 21.11.2018 gegen einen baden-württembergischen Social-Media-Anbieter eine Geldbuße von 20.000 € verhängt und nach Zusammenarbeit mit dem Unternehmen für Verbesserungen bei der Sicherheit der Nutzungsdaten gesorgt.

Das Unternehmen hatte sich am 08.09.2018 mit einer Datenpannenmeldung an den LfDI Stefan Brink gewandt, nachdem es bemerkt hatte, dass durch einen Hackerangriff im Juli 2018 Daten von ca. 330.000 Nutzenden, darunter Passwörter und E-Mail-Adressen, entwendet und Anfang September 2018 veröffentlicht worden waren. Die Nutzenden waren durch das Unternehmen gemäß Art. 34 DSGVO unverzüglich und umfassend informiert worden. Das Unternehmen legte, so der LfDI, in vorbildlicher Weise sowohl Datenverarbeitungs- und Unternehmensstrukturen als auch seine eigenen Versäumnisse offen. Das Unternehmen hatte die Passwörter der Nutzenden unverschlüsselt und unverfremdet (ungehasht), gespeichert. Die Klartextpasswörter wurden beim Einsatz eines sog. „Passwortfilters“ zur Verhinderung der Übermittlung von Nutzerpasswörtern an unberechtigte Dritte genutzt.

Das Unternehmen setzte innerhalb relativ kurzer Zeit Maßnahmen zur Verbesserung der IT-Sicherheitsarchitektur um und brachte damit die Sicherung ihrer Nutzerdaten auf den aktuellen Stand der Technik. In der wissentlichen Klartext-Speicherung der Passwörter sah der LfDI eine Verletzung des Art. 32 Abs. 1 lit a DSGVO. Wegen der „sehr guten Kooperation“ mit dem LfDI wurde durch ihn gemäß Art. 83 Abs. 4 DSGVO eine „glimpfliches“ Bußgeld verhängt, so Brink: „Wer aus Schaden lernt und transparent an der Verbesserung des Datenschutzes mitwirkt, kann auch als Unternehmen aus einem Hackerangriff gestärkt hervorgehen“ (PE LfDI Baden-Württemberg, 22.11.2018, LfDI Baden-Württemberg verhängt sein erstes Bußgeld in Deutschland nach der DS-GVO).

Baden-Württemberg

Studentische Verfassungsbeschwerde gegen Auswertung einer Backup-Datei

Am 14.01.2019 reichte die Studierendenvertretung der Albert-Ludwigs-Uni-

versität Freiburg (VS – Verfasste Studierendenschaft) Verfassungsbeschwerde gegen die Bundesrepublik Deutschland ein, um zu verhindern, dass das Bundesamt für Verfassungsschutz (BfV) eine Sicherungsdatei der VS, auf der Daten von 25.000 Freiburger Studierenden gespeichert sind, entschlüsselt und ausgewertet wird. Dem Landeskriminalamt (LKA) Stuttgart war bei Durchsuchungen im Rahmen des Verbots der Internetplattform linksunten.indymedia.org Ende August 2017, also 17 Monate zuvor, die verschlüsselte Sicherheitskopie (Backup) aller Daten der VS in die Hände gefallen. Diese waren von einem Mitarbeiter der VS extern aufbewahrt worden, was bisheriger Praxis entsprach. Der Versuch, die Auswertung der gesamten Daten der VS – wozu neben den Daten aller Studierenden auch die der Beschäftigten sowie deren kompletter Mailverkehr, inklusive Anwaltskorrespondenz, gehören – gerichtlich zu unterbinden, war zwar vor dem Verwaltungsgerichtshof Mannheim (VGH) weitgehend erfolgreich, jedoch zuletzt vor dem Oberverwaltungsgericht Berlin-Brandenburg (OVG) im vorläufigen Rechtsschutzverfahren gescheitert. Das OVG erklärte die Auswertung durch das Bundesamt für Verfassungsschutz für zulässig.

Der Verfassungsschutz ist in Amtshilfe für das LKA Baden-Württemberg mit der Entschlüsselung der Daten beauftragt worden. Es sei zwar unwahrscheinlich, dass sich auf dem genannten Datenträger für das Verbotsverfahren relevante Daten befänden, so die Gerichte, es liege aber dennoch im Bereich des Möglichen. Bisher hält die Verschlüsselung des Backups den Öffnungsversuchen stand. Die VS sieht aber mit jedem weiteren Tag ein steigendes Risiko, dass die Daten durch den Verfassungsschutz entschlüsselt werden und dieser damit uneingeschränkten Zugriff zu den Daten erhält.

Marah Mauermann, Vorstandsmitglied der Studierendenvertretung, erklärte: „Es gilt unbedingt zu verhindern, dass unsere vertraulichen Daten entschlüsselt werden. Es ist unser größtes Anliegen, die Daten der Studierenden zu schützen. Gegenüber uns wurde zu keiner Zeit ein Verdachtsmoment geäußert, noch wurde unsere Körperschaft des öffentlichen Rechts um Hilfe auf Amtswegen gebeten. Durch das anhaltende Vorgehen und die Abweisung unserer Anträge vor Gericht sehen wir die hart erkämpfte studentische Selbstverwaltung erheblich beschädigt. Wir hoffen nun, dass das Bundesverfassungsgericht den Studierenden ein Recht auf den Schutz ihrer Daten zuspricht.“

Der die VS vor dem BVerfG vertretende Berliner Jurist Prof. Dr. Ralf Alleweldt ergänzte: „Es ist völlig unverhältnismäßig, einen so umfangreichen Datenbestand ohne jede dargelegte Beweisbedeutung mit der pauschalen Begründung durchzusehen, es könne nicht ausgeschlossen werden, dass sich dort verfahrensrelevante Daten befinden, zumal das Vereinsverbot bereits erlassen ist und sich auf eine frei zugängliche Internetplattform bezieht. Die Studierendenschaft wird in ihren Rechten auch dadurch verletzt, dass ein Nachrichtendienst, das Bundesamt für Verfassungsschutz, mit der Auswertung beauftragt ist. Faktisch wird das Verbotsverfahren gegen die Internetplattform durch das Bundesamt gesteuert, das sich für seine Durchführung der Länderbehörden und seiner Polizeien bedient.“ Dies sei ein Verstoß gegen das Gebot der Trennung zwischen Polizei und Nachrichtendiensten (Vorstand StuRa Uni Freiburg, PE 18.01.2019, Angriff auf studentische Daten - Verfassungsbeschwerde eingereicht; siehe auch Kauß, Fahndung ins Blaue hinein, Bürgerrechte&Polizei, CILIP 117, November 2018, 50-56).

Baden-Württemberg

Mannheimer Polizei installiert Videoüberwachung mit Mustererkennung

Die Stadt Mannheim testet seit dem 03.12.2018 am dortigen Hauptbahnhof ein Videoüberwachungssystem mit Mustererkennung, mit dessen Hilfe Straßenkriminalität besser bekämpft werden soll. Weitere Kriminalitätsbrennpunkte sollen innerhalb der kommenden Monate und Jahre folgen. Mannheim investiert 900.000 € für das System; das Land Baden-Württemberg beteiligt sich mit weiteren 700.000 €. Mannheims Erster Bürgermeister und Ordnungsdezernent Christian Specht (CDU) sagte, dass 72 Kameras verschiedene Plätze in der Innenstadt und dem Stadtteil Neckarstadt fokussieren sollen. Getestet werde das System innerhalb der kommenden fünf Jahre.

Die Kameras erfassen die Bilder und schicken diese verschlüsselt zum polizeilichen Lagezentrum, wo sie mithilfe eines Algorithmus automatisiert ausgewertet werden. Erkennt die Software hektische oder untypische Bewegungen, etwa ein Schlagen, Rennen oder Fallen, blinkt eine Lampe auf, und eine PolizistIn schaut sich die Szene am Bildschirm an. Im Bedarfsfall soll dann eine Streife in gut zwei Minuten vor Ort sein. Polizeipräsident Thomas Köber betonte, dass BeamtInnen auf Basis der Kamerabilder die Situation bewerten und über einen Einsatz entscheiden: „Es entscheidet nicht die Maschine, es entscheidet der Mensch.“

Rechtliche Bedenken soll es angeblich nicht geben. Das jüngst geänderte Polizeigesetz des Landes stehe in Einklang mit der Anwendung der neuen Technologie. Das bestätigte Baden-Württembergs Datenschutzbeauftragter Stefan Brink. Ihm zufolge gibt es zurzeit keinen Anlass zur Kritik: „Nach wie vor ist Grundvoraussetzung, dass der überwachte Bereich als Kriminalitätsschwerpunkt identifiziert wurde, was durch entsprechende Zahlen nachzuweisen ist.“ Baden-Württembergs Innenminister Thomas Strobl (CDU) betonte: „Es geht nicht um Gesichtserkennung, sondern um das Erkennen von Verhaltensmustern.“ Zudem würden private Bereiche wie Wohnungen verpixelt. Man wolle auch keinen Datenvorrat anlegen. Daher werden Aufzeichnungen lediglich 72 Stunden aufbewahrt, dann vernichtet.

Entwickelt wurde die Software vom Fraunhofer Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) in Karlsruhe. Von einer finalen Anwendungsreife kann laut IOSB noch nicht die Rede sein. „Mit der Anwendung im öffentlichen Raum wird völliges Neuland betreten.“ Für Minister Strobl ist das Projekt dennoch jetzt schon „Pionierarbeit made in Baden-Württemberg“. Die neue Kameraüberwachung sei kein Allheilmittel. Allerdings sei sie ein wichtiges Instrument im Kampf gegen die Kriminalität.

Auch nach Polizeiangaben hat das Verfahren seine Grenzen. Man wolle nun testen, wie gut bestimmte Verhaltensmuster – etwa Schlagen oder Treten – überhaupt durch die entsprechenden Algorithmen erkannt werden können. Davon abgesehen gebe es auch noch die alte Diskussion, wonach sich im Zuge der Kameraüberwachung die kriminelle Szene in andere Bereiche – nämlich nicht überwachte Gebiete – zurückzieht.

Der stellvertretende Fraktionsvorsitzende der SPD im Stuttgarter Landtag, Sascha Binder meinte: „Wir stehen heute am Anfang eines Entwicklungsprozesses und nicht am Beginn einer volleinsatzfähigen Videoüberwachung." Mit Mustererkennung bei der Videoüberwachung wird in Deutschland auch in Berlin experimentiert, wo im Sommer 2018 das kontrovers diskutierte Pilotprojekt zur automatischen Gesichtserkennung durch Überwachungskameras am Bahnhof Südkreuz startete. Der im Oktober 2018 veröffentlichte Abschlussbericht des zweiphasigen Tests bescheinigte den Systemen Erfolg. Bundesinnenminister Seehofer (CSU) erklärte, die Technik habe sich „in beeindruckender Weise bewährt", und drängte auf eine breitere Einführung in die Polizei-Arbeit (Mannheim testet verhaltensbasierte Videoüberwachung, www.heise.de 03.12.2018, Kurzlink: https://heise.de/-4239279)

Baden-Württemberg

USB-Sticks in Uniklinik geklaut

Der Klinikumsvorstand des Universitätsklinikums Heidelberg musste betroffenen PatientInnen mitteilen, dass Mitte November 2018 aus einem verschlossenen Büro drei USB-Sticks entwendet worden. Darauf befanden sich nach Angaben einer Kliniksprecherin Namen, Geburtsdaten und Informationen zu Infektionserregern, die bei den üblichen Screeninguntersuchungen von PatientInnen festgestellt worden waren. Betroffen waren insgesamt 287 Erkrankte. Diese wurden Mitte Januar 2019 angeschrieben und über den Vorfall informiert. Dass dies zwei Monate dauerte, begründete die Kliniksprecherin damit, dass zuerst zweifelsfrei rekonstruiert werden musste, welche Daten gestohlen wurden und welche nicht. Informiert wurden auch der Datenschutzbeauftragte des Klinikums sowie der Landesdatenschutzbeauftragte, so wie es die EU-Datenschutzgrundverordnung vorschreibt. Außerdem erstattete die Verwaltung Strafanzeige gegen Unbekannt.

Die Sprecherin des Universitätsklinikums teilte mit, dass die Staatsanwaltschaft das Verfahren inzwischen eingestellt hat, da der Täter nicht ermittelt werden konnte. Man gehe inzwischen davon aus, dass es der Dieb tatsächlich nur auf die drei Datenträger im Wert von 39,30 Euro abgesehen hatte. Dass die Daten in irgendeiner Weise missbraucht wurden, ist bisher nicht bekannt. Nur zwei der angeschriebenen Patienten hatten sich mit Rückfragen an die Rechtsabteilung des Universitätsklinikums gewandt: „Wer hat heutzutage Interesse an drei USB-Sticks?", fragte ein betroffener Patient; in seinen Augen kann es nur um die Daten gegangen sein: „Das kann man sicher als Druckmittel gegen Einzelne verwenden."

Das Universitätsklinikum hat seine Mitarbeitenden nach dem Vorfall erneut darauf eingeschworen, „die Nutzung von USB-Sticks auf ein absolutes Mindestmaß zu reduzieren". Sie werden angehalten, stattdessen für die Weitergabe von Daten das interne Kliniknetz zu verwenden, so die Kliniksprecherin: „Wir arbeiten an technischen Lösungen, dass die Sticks, wenn sie unbedingt genutzt werden müssen, nur mit Verschlüsselung funktionieren" (Sommer, USB-Sticks mit Infos über Patienten gestohlen, www.rnz.de 16.01.2019).

Baden-Württemberg

GFF erhebt Verfassungsbeschwerde gegen Staatstrojaner

Die Gesellschaft für Freiheitsrechte (GFF) hat gemeinsam mit mehreren unterstützenden Organisationen und Personen eine Verfassungsbeschwerde gegen Baden-Württembergs überarbeitetes Polizeigesetz eingelegt und konzentriert sich dabei auf die Regelung zum Staatstrojaner. Dafür würden IT-Sicherheitslücken ausgenutzt, bei denen die Ermittlungsbehörden das Interesse hätten, dass diese nicht von den Herstellern geschlossen werden. Solange solche Lücken nur der Polizei, nicht aber den Herstellern bekannt seien, könnten auch Cyberkriminelle darauf zugreifen. Das sei unvereinbar mit dem Schutzauftrag des Staates gegenüber den BürgerInnen.

Unterstützt wird die GFF vom Chaos Computer Club Stuttgart, zwei Anwälten und Journalisten, einem Onlinehändler und einer Einkaufsgesellschaft für Internet-Service-Provider. Diese sehen für sich die Gefahr von Cyberangriffen sowie für die Rechte von Dritten, beispielsweise MandantInnen. Formuliert wurde die Verfassungsbeschwerde von Tobias Singelnstein von der Ruhr-Universität Bochum. Zur Finanzierung des Rechtsstreits ruft die GFF öffentlich zu Spenden auf. Insgesamt seien 25.000 Euro nötig.

Anfang Oktober 2018 hatte die GFF bereits angekündigt, gemeinsam mit Partnern Verfassungsbeschwerde gegen die Reform des bayerischen Polizeiaufgabengesetzes (BayPAG) einzulegen. Auch dabei geht es u. a. um den Staatstrojaner. Die GFF will ebenso gegen ähnliche Regelungen in anderen Bundesländern vor das Bundesverfassungsgericht nach Karlsruhe ziehen (Holland, Staatstrojaner: Verfassungsbeschwerde gegen Baden-Württembergs Regelung, Kurzlink: https://heise.de/-4245429).

Bayern

Keine Weihnachtshilfe für Arme wegen „Datenschutz"

RTL regte sich auf: „Kein Geschenke-Geld wegen Datenschutz! Kann das wirklich wahr sein? Ja, leider." Viele arme Kinder im bayerischen Holzkirchen sollten Weihnachten 2018 leer ausgehen. Seit 30 Jahren schenkte die Gemeinde den bedürftigen Familien ein Extra-Weihnachtsgeld, damit auch ihre Kinder etwas zum Auspacken bekommen. Jetzt sollte damit Schluss sein. Als Grund wurde die neue Datenschutz-Grundverordnung angegeben. Wegen

den Bestimmungen der DSGVO dürfe das Sozialamt des Landratsamtes Miesbach Namen und Adressen von Sozialhilfeleistungs-EmpfängerInnen nicht wie früher an das Holzkirchner Rathaus weitergeben.

Entsprechend sauer reagierte der Bürgermeister der 16.000-Einwohner-Gemeinde im Landkreis Miesbach südlich von München, Olaf von Löwis: „Ein bürokratisches Monster (...), das an der Praxis vorbeigegangen ist." Er könne sich nicht vorstellen, dass einer der Menschen, die in der Vergangenheit Geld bekommen haben, ein Problem damit hätte, wenn die Gemeinde dessen Adresse wüsste.

So leicht kann Datenschutz zum Buhmann gemacht werden. Tatsächlich versteckte sich das Landratsamt nur mit seiner geistigen und sonstigen Faulheit: Die Rechtslage hat sich gemäß den Sozialgesetzbüchern (SGB) mit der DSGVO nicht geändert. Es wäre auch unbürokratisch möglich, nach alter und neuer Rechtslage die Daten auf Zustimmungsbasis weiterzugeben. Nur würde das voraussetzen, dass die BürokratInnen im Landratsamt tätig würden (Datenschutz-Irrsinn in Bayern: Arme in Holzkirchen kriegen kein Extra-Weihnachtsgeld mehr, rtlnext.rtl.de 23.11.2018).

Bayern

DSGVO verhinderte auch Wunschzettel am Weihnachtsbaum

Die Umsetzung der seit Mai 2018 geltenden Datenschutz-Grundverordnung (DSGVO) treibt mitunter merkwürdige Blüten, so auch im fränkischen Roth: Kinder konnten 2018 keine Wunschzettel mehr an dem Weihnachtsbaum auf dem Christkindlesmarkt hinterlassen. Die Stadtverwaltung der Kreisstadt nahe Nürnberg hatte diese beliebte Advents-Aktion abgesagt. Die Stadt Roth befürchtete, mit den Wunschzetteln gegen die DSGVO zu verstoßen und damit eine Strafe zu riskieren, so der städtische Veranstaltungsorganisator Andreas Kowohl: „Früher haben Kinder ihre ausgefüllten Wunschzettel einfach an den Christbaum gehängt." Dort hingen die Wunschzettel dann den Advent über, mitten auf dem historischen Marktplatz von Roth. „Die Zettel waren offen für jeden einsehbar", nicht nur der Wunsch des Kindes, sondern auch Name, Alter und Adresse. „Das sind sensible Daten, die können wir nicht einfach so weitergeben."

Genau das passierte in der Vergangenheit mit den rund 4.000 Wunschzetteln, die in Roth jedes Jahr zusammen kamen: Die Stadt hat die Zettel an diejenigen Partner und Sponsoren weitergegeben, die bei der Erfüllung des jeweiligen Wunschs behilflich sein konnten. An die Buchhändler etwa, wenn ein Buchwunsch auf dem Zettel stand. Oder an die Polizei, wenn der Herzenswunsch eine Fahrt im Polizeiauto war. Um in Sachen Datenschutz auch der neuen Verordnung gemäß auf Nummer sicher zu gehen, fragten die Marktveranstalter bei dem städtischen Datenschutzbeauftragten nach. Dessen Antwort: Um nicht gegen die DSGVO zu verstoßen, müssten die Kinder mehrere kleinbedruckte DIN A4-Seiten voller juristischer Formulierungen ausfüllen. Dies kommentierte Andreas Kowohl von der Stadt Roth: „Das können die Kinder ja gar nicht. Und das wollen auch wir nicht – wir wollen eine unkomplizierte Lösung." Bis zum Advent 2019 soll nun eine neue, datenschutzkonforme Lösung her, damit Rother Kinder im kommenden Jahr wieder Wunschzettel an den Christbaum hängen können, so Andreas Kowohl: „Denn die Aktion hat ja auch den Reiz des Marktes ausgemacht" (DSGVO sorgt für nächstes Chaos - Wunschzettel-Aktion für Kinder zu Weihnachten gestoppt, wize.life 16.11.2918).

Berlin

Datenschutzbeauftragte angeblich für AfD-Lehrerdenunziation unzuständig

Berlins Beauftragte für Datenschutz, Maja Smoltczyk, hat sich zwar gegen die Überwachung des AfD-Portals „Neutrale Schule" ausgesprochen, meinte aber, diese falle nicht in ihre „Kontrolltätigkeit". Dies ergibt sich aus einem Brief Smoltczyks an die Berliner Bildungssenatorin Sandra Scheeres (SPD), die Smoltczyk um Prüfung gebeten hatte, ob Daten, die in dem Portal über Menschen gesammelt werden, an Dritte weitergegeben würden. Auf der Internetseite können SchülerInnen und Eltern mitteilen, wenn sich Lehrkräfte im Unterricht kritisch zur AfD äußern. Die Partei will damit nach eigener Darstellung zur Durchsetzung des Neutralitätsgebots an den Berliner Schulen beitragen (DANA 4/2018, 196 ff.). Scheeres hatte dazu aufgerufen, bei dem Portal nicht mitzumachen.

KritikerInnen sehen in dem Portal eine Plattform zur Denunziation. Auch die Datenschutzbeauftragte Smoltczyk sieht diese Gefahr, argumentiert dem Bericht zufolge aber, dass Fraktionen im Abgeordnetenhaus bei der „Wahrnehmung parlamentarischer Aufgaben" vom Berliner Datenschutzgesetz ausgenommen seien und so Personendaten verarbeiten dürften. Scheeres sieht dies anders: „Es ist doch keine parlamentarische Aufgabe, wenn eine Partei einen elektronischen Pranger gegen Berliner Lehrkräfte betreibt." Auch die Gewerkschaft Erziehung und Wissenschaft (GEW) zeigte sich unzufrieden mit der Antwort Smoltczyks (Datenschützerin will AfD-Lehrerportal nicht überwachen, www.berliner-zeitung.de 18.11.2018).

Berlin

Benachrichtigung über Funkzellen-Abfragen

Die Landespolitik führt in Berlin ein System ein, mit dem BürgerInnen künftig besser informiert werden, wenn ihre Handydaten in Ermittlungsverfahren erfasst wurden. Um Kriminelle zu fassen, wird oft überprüft, welche Handys in einer Funkzelle registriert waren. Betroffen sind von dieser Maßnahme auch die Handydaten Unverdächtiger. Justizsenator Dirk Behrendt (Grüne) wies am 13.11.2018 darauf hin, dass es bundesweit kein Transparenzsystem gibt. Berlin sage als erstes Bundesland zu, dass diejenigen, die wollen, informiert werden: „Wir betreten da bürgerrechtliches Neuland." 2017 wurden in Berlin demnach mehr als 59 Millionen Datensätze erhoben, davon 15,2 Millionen Telefonate.

BürgerInnen können sich ab sofort in dem „Transparenz-System" nur mit ihrer Handynummer anmelden. Sie erhalten dann künftig per SMS nach Abschluss eines Ermittlungsverfahrens Bescheid, wenn die eigene Mobilfunknummer in der Abfrage erfasst wurde. Danach sollen die Daten gelöscht werden. Bei der Funkzellenabfrage fordern die Ermittelnden von den Telekommunikationsanbietern alle Handydaten an, die zu einem bestimmten Zeitraum im Bereich einer bestimmten Funkzelle registriert wurden, um Straftäter zu identifizieren. Das Verfahren ist umstritten, weil dabei auch Mobiltelefone unbescholtener BürgerInnen ohne deren Wissen erfasst werden.

Behrendt betonte, bei Demonstrationen gebe es keine Abfrage von Handydaten: „Wir sind ja hier nicht in Sachsen." Gerechnet wird mit einer fünfstelligen Zahl von Anmeldungen. Im Probebetrieb hatten sich 800 Testende angemeldet. 2017 hatten Berliner Strafverfolger 474 Funkzellenabfragen durchgeführt. Die Abfrage wurde laut Justiz in 426 Ermittlungsverfahren angewandt. Die Methode kam bei Ermittlungen zu Mord, Totschlag, Raubtaten oder schwerem Diebstahl zum Einsatz.

Funkzellenabfragen sind in der Strafprozessordnung geregelt. Sie müssen demnach von der Staatsanwaltschaft beantragt und von einem Richter genehmigt werden. Laut Justiz gibt es in Berlin einige Tausend Funkzellen. Laut Richter Ulf Buermeyer, der das System maßgeblich entwickelt hat, ist mit Benachrichtigungen frühestens Mitte 2019 zu rechnen. Bislang sei nicht vorgesehen, dass über die konkreten Ermittlungen informiert wird, es solle nur ein Aktenzeichen angegeben werden: „Wir wollen die Menschen nicht beunruhigen", wenn ihre Handydaten z. B. in Mordermittlungen erfasst wurden. Die BürgerInnen sollen aber erfahren, wann und wo ihr Gerät erfasst wurde.

Die oppositionelle Berliner FDP-Fraktion monierte, statt aufwendiger technischer Verfahren müsste die menschliche Seite der Ermittlungen gestärkt werden. Gemäß Innenexperte Marcel Luthe werden mehr PolizistInnen gebraucht, die Verdächtige observieren, statt die Bewegungsdaten von Millionen Unverdächtiger systematisch zu erfassen (Funkzellen-Abfrage in Berlin soll transparenter werden, www.heise.de 13.11.2018).

Berlin

Mit Herzschlagdetektor gegen Ausbruchversuche

Nach einem spektakulären Ausbruch aus dem Berliner Gefängnis Tegel Anfang Februar 2018 wird dort jetzt mit hochsensibler Technik kontrolliert. Der Berliner Justizsenator Dirk Behrendt (Grüne) teilte mit: „Der erste Herzschlagdetektor ist im Einsatz". In jedem Fahrzeug, das die Haftanstalt verlässt, erfasst das 150.000 € teure Gerät in Sekundenschnelle menschliche Geräusche. Damit soll erkannt werden, wenn sich ein Gefangener herausschmuggelt. Einem Gefängnisinsassen in Tegel war es gelungen, in einen Lieferwagen zu klettern und unbemerkt nach draußen zu kommen. Bei der Ausfahrt-Kontrolle des Fahrzeugs war der Ausbrecher nicht erfasst worden. Später wurde er in Belgien festgenommen. Die Flucht hatte den Senator in Erklärungsnot gebracht. Es war das zehnte Mal innerhalb von sechs Wochen, dass Häftlinge aus einem Berliner Gefängnis entkamen. Alle kehrten wieder zurück oder wurden gefasst. Bis zum Jahresende 2019 sollen auch die Haftanstalten in Moabit, Plötzensee, Heidering, die Jugendstrafanstalt sowie das Frauengefängnis ausgestattet werden. Insgesamt ist der Einsatz von zwölf Geräten geplant. Die Kosten wurden mit 1,8 Mio. € veranschlagt. Gemäß Behrendt lässt sich der Herzschlagdetektor nur mit einem Training überlisten, bei dem das Herz kurzfristig aussetzt (Erster Herzschlagdetektor in Berliner Gefängnis, www.morgenpost.de 20.01.2019; Detektor gegen Ausbrecher, SZ 21.01.2019, 8).

Brandenburg

Massive Kritik am Entwurf für das Polizeigesetz

Brandenburg plant nach Nordrhein-Westfalen, Bayern, Baden-Württemberg und Hessen, sein Polizeigesetz (PolG) aufzubohren und den Ermittlern u. a. eine Befugnis zum Einsatz von Staatstrojanern für das Abhören von Messenger-Diensten und Internet-Telefonie einzuräumen. Sachverständige warnten am 07.01.2019 in einer Anhörung zu dem Gesetzentwurf im Innenausschuss des Landtags in Potsdam vor den verfassungsrechtlich problematischen Konsequenzen.

Fredrik Roggan von der Fachhochschule der Brandenburger Polizei kritisierte, dass die Lizenz zur Quellen-Telekommunikationsüberwachung mit einem Recht der Fahndenden zur „heimlichen Wohnungsdurchsuchung" einhergehe. Dies sei ein absolutes Novum. Dabei handle es sich um „mehr als ein Betretungsrecht wie beim großen Lauschangriff", sodass die Eingriffsintensität der an sich bereits fraglichen Methode noch erheblich erhöht würde. Es gebe keine Untersuchungen, wie sich ein solches Vorgehen auf Betroffene auswirken kann. Die psychologischen Folgen dürften wohl ähnlich wie bei einem Wohnungseinbruchsdiebstahl sein.

Der entsprechende § 28e PolG-E sieht Einschnitte in das in Artikel 13 GG festgelegte Recht auf Unverletzlichkeit der Wohnung von Personen vor, die mit dem Brandenburg-Trojaner ausgespäht werden sollen. Es könnte erforderlich sein, Wohnungen zu durchsuchen, um die ins Visier genommenen IT-Systeme „etwa in Schränken und ähnlichem" zu finden, meint die Regierung. Art. 13 GG erlaube aber „explizit keine heimlichen Maßnahmen", hielt Roggan dem entgegen. Solche würden „auch in keinem Kommentar erwogen". Die Klausel wäre damit „deutlich und unumstritten verfassungswidrig". Die Quellen-TKÜ soll sich auf laufende Kommunikation beschränken. Zugleich heiße es, dass ein Zugriff auf das übrige System nicht zulässig sei. Roggan meinte, dass an diesem Punkt eine „saubere technische Trennung gerade nicht möglich ist". Zudem gebe es auf Bundesebene bereits eine weite Befugnis zur Quellen-TKÜ zur Strafverfolgung, die sich nicht hinreichend von der in Brandenburg für die Gefahrenabwehr geplanten abgrenzen lasse.

Ulf Buermeyer von der Gesellschaft für Freiheitsrechte (GFF) warnte vor den gesellschaftlichen Folgen einer „Kultur der kalkulierten IT-Unsicherheit". Er

verwies dabei auf den „Ausbruch des WannaCry-Trojaners“. Die NSA habe damals eine Sicherheitslücke in Windows-Betriebssystemen geheim gehalten, die daher nicht geschlossen werden konnte und später von Kriminellen für einen Erpressungs-Trojaner ausgenutzt wurde. Der wenige Tage vor der Anhörung publik gewordene Datenklau bei Prominenten (siehe den Beitrag von Roth in diesem Heft) habe erneut gezeigt, „welches Drohpotenzial und welche Gefahr von Sicherheitslücken und mangelhafter IT-Sicherheit ausgeht“.

§ 28e des Entwurfs stelle in keiner Weise sicher, dass die „Überwachungssoftware Mindestanforderungen an die Datensicherheit und Resistenz gegen Manipulationsversuche erfüllt“. Er schaffe vielmehr „ein massives Interesse für Sicherheitsbehörden, die Cyber-Sicherheit weltweit zu schwächen“, um Systeme von Zielpersonen gegebenenfalls „hacken“ zu können. Es sei auch kaum ein Fall denkbar, in dem eine der Polizei bekannte terroristische Gefahr nicht bereits durch bestehende Kompetenzen abgewehrt werden könnte.

Wie keine andere Ermittlungsmethode erlaubt es die Quellen-TKÜ laut Buermeyer, „Menschen zum Objekt der Ausspähung zu machen“. Gegen keine andere Methode seien Verdächtige so wehrlos, denn der direkte Zugriff auf das System diene gerade dem Zweck, Verschlüsselungsverfahren zu umgehen und den informationellen Selbstschutz ins Leere laufen zu lassen. Keine andere Ermittlungsmethode biete so „insgesamt ein vergleichbares totalitäres Potential“. Die geplanten Regeln seien vor diesem Hintergrund „insgesamt verfassungsrechtlich wie rechtspolitisch deutlich misslungen“.

Auch die brandenburgische Datenschutzbeauftragte Dagmar Hartge meinte, dass vom Staatstrojaner enorme Gefahren ausgehen. Mit der damit einhergehenden Infiltration eines Smartphones oder Rechners sei „die entscheidende Hürde genommen, um das System insgesamt auszuspähen“. Generell weite der Regierungsentwurf polizeiliche Datenverarbeitungsbefugnisse deutlich aus und werfe „erhebliche freiheits- und datenschutzrechtliche Bedenken auf“.

So solle etwa ein „nicht konkretisierter Gefahrenbegriff“ als Eingriffsschwelle für polizeiliches Handeln eingeführt werden. Sie habe „erhebliche Zweifel, dass diese Änderung noch verfassungsmäßig ist“. Es entstehe der Eindruck, „dass das Polizeirecht immer weiter dem Recht des Verfassungsschutzes angeglichen werden“ solle. Mit der „zeitlichen Vorverlagerung der Eingriffsbefugnisse“ werde zudem der betroffene Personenkreis enorm ausgeweitet. Die „Kumulation neuer Befugnisse und das Herabsenken der Einschreitschwellen“ erhöhen Hartge zufolge die Datenmengen auf ein Besorgnis erregendes Ausmaß. Dies werfe die Frage auf, „ob Brandenburg mit dem Gesetzentwurf nicht bereits nahe an eine flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten herankommt“. So würde etwa die erweiterte, zweiwöchige Speicherfrist bei der Videoüberwachung „eine Vielzahl unbeteiligter Personen über einen langen Zeitraum betreffen, die sich lediglich an einem der benannten Orte aufhalten, ohne dass sie selbst im Zusammenhang mit der Straftat stehen oder selbst eine begangen hätten“. Auch der Einsatz von Bodycams müsse zunächst getestet und evaluiert werden. Das geplante „Pre-Recording“ von 60 Sekunden in einem Kurzzeitspeicher sei verfassungsrechtlich „äußerst problematisch“.

Praktiker wie Nils Kößler aus dem Landespolizeipräsidium Hessen oder der frühere Berliner Polizeipräsident Klaus Kandt bezeichneten das Vorhaben dagegen als zwingend erforderlich und ausgewogen. Allenfalls sei zu überlegen, ob die vorgesehene Schleierfahndung noch ausgeweitet werden sollte. Wenn diese auf einzelne Hauptverkehrswege beschränkt bleibe, könne sich eine Lücke öffnen. Zudem sollte klargestellt werden, dass die Polizei auch virtuelle Währungen pfänden dürfe. Thomas Bode vom Bund deutscher Kriminalbeamter (BDK) meinte, dass der Entwurf zu stark auf die Terrorabwehr ausgerichtet sein könnte und größere Bedrohung für Heranwachsende wie Crystal Meth außen vor lasse. Die Abgeordneten wollen das Dossier nun weiter beraten und vor einem Beschluss voraussichtlich im März 2019 gegebenenfalls noch mögliche Korrekturen festzurren. (Krempl, Polizeigesetz Brandenburg: Scharfe Kritik an heimlicher Wohnungsdurchsuchung, www.heise.de 09.01.2019, Kurzlink: https://heise.de/-4270176)

Bremen

Kirchenwahlen diesmal „nichtöffentlich“

Im Bistum Hildesheim wurden am 10. und 11.11.2018 die Kirchenvorstände und Pfarrgemeinderäte neu gewählt. Damit waren auch die etwa 17.500 Katholiken in den drei Gemeinden des Dekanats Bremen-Nord aufgerufen, über die Zusammensetzung der Gremien für die kommenden vier Jahre zu entscheiden.

Zu unterschiedlichen Interpretationen haben die aktuellen Datenschutzbestimmungen geführt. Die KandidatInnen mussten eine Erklärung für die Bekanntgabe ihrer Bewerbung abgeben, die aber nur eine gemeindeinterne Bekanntgabe der Namen erfasste. In einem Fall wurde die Bewerberliste aus dem Schaukasten der Gemeinde entfernt und dann im Kircheninnern ausgehängt. Eine andere Gemeinde strich alle Wohnortangaben von den Listen. Dennoch fanden sich von zwei Pfarreien die Kandidatenlisten mit Fotos im Internet wieder. Die Richtlinien des Datenschutzes hatten auch Auswirkungen auf die Bekanntgabe der Wahlergebnisse. Diese erfolgte in den Gottesdiensten, anschließend durch einen Aushang in den Kirchen. Eine öffentliche Bekanntmachung der Listen der Gewählten war zumindest in einer der drei Pfarreien nicht vorgesehen (Schwarz, Probleme mit dem Datenschutz, www.weser-kurier.de 06.11.2018).

Hessen

Schwarz-Grün für IP-Tracking und mehr Videoüberwachung

Nach rund vierwöchigen Verhandlungen haben CDU und Grüne in Hessen am 19.12.2018 ihr Programm für die geplante zweite gemeinsame Regierungsperiode veröffentlicht. Ein Schwerpunkt des Koalitionsvertrags für die Zeit bis 2023 liegt auf der Digitalisierung, in die eine Milliarde Euro fließen soll. Ein

grüner Anstrich ist in der Innen- und Rechtspolitik kaum erkennbar.

Um die Sicherheit im Land zu stärken, sollen die hessische Justiz und Polizei „personell und sachlich ausgebaut und mit weiteren rechtlichen Möglichkeiten ausgestattet“ werden. Dazu zählen die Koalitionspartner unter anderem das „IP-Tracking“, das sie einführen wollen, um „Anschlags- und Amokgefahren“ besser verhindern zu können. Damit sollen verdächtige Internetnutzende identifizierbar werden. Ermittlungsbehörden versenden hierzu unter fremder Flagge eine E-Mail mit einer verdeckten, etwa in transparente Grafik-Pixel eingebauten Lesebestätigungsfunktion. Öffnet der Adressat die Nachricht, wird die aktuelle IP-Adresse des Internetanschlusses übertragen. Schwarz-Grün will die Videoüberwachung „an besonderen Gefahrenorten“ wie Flughäfen, Bahnhöfen, Sportstätten, Einkaufszentren oder Packstationen ausbauen. Vor allem im Kampf gegen den Terrorismus müssten weitere gesetzliche Verschärfungen geprüft werden. Das gelte vor allem im Umgang mit „Gefährdern“.

Neue Instrumente wie spezielle Datenverarbeitungssysteme, die bereits vorhandene Informationen aus polizeilichen Datenbanken bündeln und auswerten, können laut Vertrag „bei der Bewältigung aktueller polizeilicher Herausforderungen von großem Nutzen sein“. Schwarz-Grün will an „hessenDATA“ der US-Firma Palantir zur Big-Data-Analyse festhalten. Nach einer Systemevaluierung soll allein geprüft werden, ob der Katalog der Straftaten, bei dem die Software eingesetzt werden kann, „angepasst werden soll“.

Bürgerrechtsorganisationen wie z. B. Digitale Gesellschaft hatten im Vorfeld der Koalitionsverhandlungen dafür geworben, die mit der jüngsten Reform des Polizeirechts geschaffenen Lizenzen für den Einsatz des Hessentrojaners zur heimlichen Online-Spionage und elektronischer Fußfesseln zurückzunehmen, da damit die Demokratie gefährdet werde. Davon ist in dem Vertrag keine Rede. Beide Parteien wollen vielmehr „neue Befugnisse“ für die Fahnder schaffen und dabei nur deren „Notwendigkeit nach den Prinzipien der Rechtsstaatlichkeit, Verhältnismäßigkeit und Wirksamkeit“ prüfen.



Eine Ausstattungsoffensive soll die Ermittlungsbehörden „technisch auf ein noch höheres Niveau“ bringen. Dazu gehörten „Bodycams in allen Dienststellen“ sowie „weitere Distanz-Elektroimpulsgeräte“ („Taser“). Die Einsatzkräfte würden künftig „mit Tablets, Handys und modernen Software-Apps ausgestattet, die Lagebilder, Ermittlungsinstrumente und vor allem Auskunftssysteme beinhalten“.

Die parlamentarische Kontrolle des Verfassungsschutzes soll gestärkt werden. Deutlich verkürzen will die Koalition bei dieser Behörde die bisherigen „pauschalen Einstufungsfristen für Verschlusssachen von 90 oder 120 Jahren“. Um Kinder im Internet besser zu schützen, will die Koalition „den Strafrahmen für den Besitz von Kinderpornographie auf eine Freiheitsstrafe von bis zu fünf Jahren erhöhen“. Handy-Nutzende müssten beim Kauf von Prepaid-Karten oder Vertragsabschluss identifizierbar sein. Es soll eine Rechtsgrundlage geschaffen werden, um „grenzüberschreitend beweiserhebliche Daten“ sichern und im Ausland gespeicherte Informationen „auch in hier geführten Gerichtsverfahren verwerten zu können“ (eEvidence).

Die Koalition will das „Internet der Dinge“ sicherer machen sowie europaweit verpflichtende Mindestanforderungen an die IT-Sicherheit und ein gültiges Zertifizierungssystem vorantreiben. Die Anbieter softwarebasierter Alltagsgeräte sollen verpflichtet werden, regelmäßig Updates anzubieten. Schwarz-Grün erwägt eine „schwarze Liste“ über Hersteller und Produkte, „die korrumpiert wurden“. Dazu kommen soll eine „Haftung der Verantwortlichen für Produkte Künstlicher Intelligenz“ (KI), wenn daraus „Rechtsverstöße resultieren“.

CDU und Grüne sorgen sich um die Cybersicherheit: „Die Wettbewerbsfähigkeit der hessischen Wirtschaft wird durch gezielte Spähangriffe fremder Nachrichtendienste und internationale Konkurrenz großen Gefahren ausgesetzt. Daher gründen wir eine schnelle Notfall-Eingreiftruppe (Computer Emergency Response Team), um bei digitalen Sicherheitsvorfällen schnell reagieren zu können.“ Zudem ist ein landeseigenes IT-Sicherheitsgesetz geplant.

„Hate-Speech treten wir konsequent entgegen, stärken die Arbeit des Demokratiezentrums und schaffen ein ‚Netzwerk Prävention‘.“ „Extremisten jedweder Art treffen in Hessen auf unseren erbitterten Widerstand.“ Bedeutende Ermittlungsverfahren wegen Hasskriminalität im Netz sollen landesweit durch Spezialisten der Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) bearbeitet werden, die zu diesem Zweck „personell und materiell aufgestockt wird“. Mit einem Modellprojekt unter dem Motto „Verfolgen statt nur Löschen“ will die Koalition „einer zunehmenden Verrohung der Debattenkultur entschieden entgegentreten“.

Digitalisierung bedeutet laut Koalitionsvertrag ferner, „die informationelle Selbstbestimmung der Menschen zu sichern, den Datenschutz zu stärken und Verbraucherrechte auch online zu gewährleisten“. Digitale Techniken müssten „vom Nutzen für die Menschen gedacht“ werden. Dies fange „bei der Versorgung mit schnellem Internet und Mobilfunk an“ und reiche „über die technische und inhaltliche Vorbereitung unserer Schulen und Hochschulen auf die digitale Welt bis hin zu einer öffentlichen Verwaltung“, die für BürgerInnen bequem sowie barrierefrei rund um die Uhr online übers Web und mobil erreichbar sei.

Langfristig strebt Schwarz-Grün „ein möglichst flächendeckendes 5G-Netz“ und einen „Ausbau der WLAN-Verfügbarkeit“ an. „In einem ersten Schritt werden wir freien Internetzugang in allen öffentlichen Gebäuden des Landes ermöglichen“. Bis 2025 soll Hessen „durch die Umsetzung der Gigabitstrategie“ flächendeckend mit leistungsfä-

higen Infrastrukturen versorgt sein. Um diese Vorhaben zu verwirklichen, ist in dem Land erstmals ein von der CDU geführtes eigenständiges Digitalministerium vorgesehen.

Die Koalition will Unternehmensgründer fördern und eine Startup-Initiative landesweit umsetzen. Mit einem Wachstumsfonds für Wagniskapital soll Hessen „Zentrum für Innovation und Entwicklung" werden. Die „Maßnahmen zur Unterstützung der Kultur- und Kreativwirtschaft" soll mit einer neuen „Indie-Games-Messe" für kleine und unabhängige Spieleentwickler verstärkt werden. Der Markt für Online-Glücksspiel in Deutschland soll „endlich rechtlich wie faktisch kohärent" reguliert werden.

Den öffentlich-rechtlichen Rundfunk bezeichnet die Koalition als „unverzichtbare Säule unserer freiheitlich demokratischen Grundordnung". In einer digitalen Medienwelt, in der die Abgrenzung zwischen Fakten und Meinungen, Inhalt und Werbung und die Beurteilung der Glaubwürdigkeit von Quellen immer schwieriger werde, komme ihm eine bedeutsame Rolle zu: „Gäbe es den öffentlich-rechtlichen Rundfunk nicht, man müsste ihn angesichts der Zustände in der Welt und der Anfeindungen von Links- und Rechtsaußen erfinden." CDU und Grün wollen daher eine Bestands- und Entwicklungsgarantie für ARD, ZDF und den Deutschlandfunk. Als „dritte Säule" gehöre dazu ein „öffentlich-rechtliches und zeitlich unbegrenztes, werbefreies Telemedienangebot im Internet" (Krempl, Hessen: Schwarz-Grün will IP-Tracking, Taser und mehr Videoüberwachung, www.heise.de 20.12.2018, Kurzlink: https://heise.de/-4257763).

Hessen

Verdacht der Datenweitergabe von Polizei an Rechtsextreme

Nach der Suspendierung von fünf Frankfurter Polizeibeamten, die einen rechtsradikalen Chat betrieben hatten und die verdächtigt werden, interne Daten aus dem Polizeicomputer über eine türkischstämmige Anwältin herausgegeben zu haben, wurde Anfang 2019 ein weiterer Fall bekannt, in dem ein Polizist unrechtmäßig interne Daten an ein bekennendes Mitglied einer Neonazi-Vereinigung herausgab. Ermittelt wird gegen einen Polizisten aus Osthessen, dem vorgeworfen wird, eine Bekannte aus der gewaltbereiten Neonazigruppe „Aryans" mit Daten versorgt zu haben. Dies wurde in einem Prozess gegen zwei hessische „Aryans"-Mitglieder bekannt, der am 10.01.2019 in Sachsen-Anhalt begonnen hat.

Die „Aryans" stehen der bundesweit organisierten gewaltbereiten Neonazivereinigung „Division Braune Wölfe" nahe. Den beiden Angeklagten wird vorgeworfen, am 01.05.2017 in Halle (Saale) mit ihrem Auto wehrlose Menschen gejagt und mit Steinen und Flaschen beworfen zu haben. Carsten M. soll zwei Wanderer mit einem Starkstromkabel auf den Kopf geschlagen und schwer verletzt haben. Bei den Ermittlungen gegen eine der beiden Angeklagten wurde auch deren Handy ausgewertet. Darin findet sich neben Nazipropaganda und Ausführungen zu den Taten in Halle („Zecken verdroschen") auch ein Chatverlauf, in dem sie einen ihr bekannten hessischen Polizeibeamten zweimal darum bittet, aus dem internen polizeilichen Informationssystem Daten für sie abzurufen. Der Polizist kam der Bitte gemäß Stand der Ermittlungen nach. Um welche Informationen es sich genau handelt, die der Polizist herausgab, wurde in Halle nicht bekannt.

Laut Gewerkschaft der Polizei (GdP) wechselte der Polizist vor zwei Jahren nach Niedersachsen. Den hessischen Sicherheitsbehörden lägen keine Erkenntnisse vor, dass der betroffene Beamte aus rechtsextremistischen Motiven gehandelt habe. Die Auswertung eines Chatprotokolls zwischen dem Tatverdächtigen und einer weiteren Person ließen vielmehr darauf schließen, dass der Beamte diese Person vor den Rechtsextremisten warnen wollte.

Dieser Vorgang erinnert an die Vorfälle einer rechtsextremistischen Chatgruppe im 1. Polizeirevier in Frankfurt/Main rund um die Frankfurter Anwältin Seda Başay-Yıldız. Sie hatte im August 2018 einen Drohbrief bekommen, unterzeichnet mit dem Namen „NSU 2.0". Die Anwältin hat fünf Jahre lang im NSU-Prozess die Angehörigen eines Mordopfers vertreten. Sie verteidigt auch in Islamisten-Prozessen. In dem Drohschreiben an sie waren höchstpersönliche Daten wie der Name ihrer kleinen Tochter sowie ihre Privatadresse verzeichnet, Daten, die es nur im Einwohnermeldeamt oder im Polizeicomputer gibt. Der Briefschreiber drohte ihr an, man werde ihre zweijährige Tochter „abschlachten". So hieß es in dem Brief: „Verpiss dich lieber, solange du hier noch lebend rauskommst, du Schwein!"

Die Ermittlungen in diesem Fall haben ergeben, dass die privaten Daten der Anwältin in einer Frankfurter Polizeiwache aus dem Computer abgerufen worden waren, obwohl es dafür keinerlei Notwendigkeit gab. Die fünf verdächtigen Polizisten tauschten offenbar wochenlang rassistische Nachrichten aus. Sie schickten sich Hitler-Bilder und Hakenkreuze per Computer. Gegen die vier Polizisten und eine Kollegin wird wegen Volksverhetzung ermittelt. Sie sind vom Dienst suspendiert. Auch gegen einen weiteren Polizisten in Marburg laufen Ermittlungen. Die Ermittlungen schienen keine nachhaltige abschreckende Wirkung zu haben: Mitte Januar 2019 wurde bekannt, dass Başay-Yıldız am 20.12.2018 erneut ein Fax bekam, das sich wieder auf interne Daten aus dem Polizeicomputer stützt, obwohl die Polizisten aus der Frankfurter Wache vom Dienst suspendiert waren. Es nennt den Namen des Vaters, des Mannes und der Tochter der Anwältin – alles Menschen, die unter ihrer Adresse gemeldet sind. Nach ihrer Aussage sind dies alles Angaben, die „man nicht über die sozialen Netzwerke herausfinden" kann: „Und mein Vater ist 79; der ist nicht auf Facebook oder sonstwo aktiv." Der Faxbrief bezieht sich klar auf die Suspendierung der Frankfurter Polizisten: „Dir hirntoten Scheißdöner ist offensichtlich nicht bewusst, was du unseren Polizeikollegen angetan hast! Allerdings kommt es jetzt richtig dicke für dich, du Türkensau! Deine Scheiß (Name der Tochter) reißen wir den Kopf ab … und der Rest eurer Dönercrew wird ebenfalls kompetent betreut." Wieder steht am Ende NSU 2.0. Başay-Yıldız bekam daraufhin wieder Besuch von der Polizei, die ihr versicherte, es bestehe keine Gefahr für sie. Gleichzeitig haben sie ihr angeboten, einen Waffenschein zu besorgen,

falls sie sich zu ihrem eigenen Schutz bewaffnen wolle, was sie kommentierte: „Ich soll mich bewaffnen? In Deutschland? Nur, um meiner Arbeit als Anwältin nachzugehen?“ Sie dachte, für den Schutz der BürgerInnen sei die Polizei zuständig. Damit nicht genug. Im Januar 2019 erhielt die Anwältin weitere Faxe im selben Stil und mit rassistischen Schmähungen, die augenscheinlich von demselben Absender stammen.

Ob zwischen den Frankfurter Polizisten und dem in dem Prozess in Halle bekannt gewordenen Fall eine Verbindung besteht, ist unklar. Die innenpolitische Sprecherin der Grünen-Bundestagsfraktion Irene Mihalic forderte umfassende Aufklärung. Der Fall zeige erneut, dass solche Vorfälle nicht vorschnell als Einzelfälle bezeichnet werden dürften (Ramelsberger, Hilfe aus dem Polizeicomputer, SZ 11.01.2019, 5; Decker, Hat Polizist Neonazis mit Daten versorgt? Kieler Nachrichten 12.01.2018, 4; Ramelsberger, „Kopf ab“ SZ 14.01.2019, 1; Steinke, Hessens Polizei in neuer Bedrängnis, SZ 30.01.2019, 1).

Niedersachsen

Hoheitliche Videokontrolle in Schlachthöfen?

Niedersachsens Landwirtschaftsministerin Barbara Otte-Kinast (CDU) erwägt, rechtlich die Überwachung von Schlachthöfen durch Videokameras vorzuschreiben, um die Einhaltung des Tierschutzrechts zu überprüfen, so eine Sprecherin ihres Hauses: „Die Ministerin lässt derzeit juristisch prüfen, welche Möglichkeiten es gibt, verbindlich ein Kamerasystem in den Bereichen der Anlieferung, des Zutriebes, der Betäubung und der Schlachtung der Schlachthöfe anzuordnen.“

Ende 2018 werteten zehn Mitarbeitende des Vereins Deutsches Tierschutzbüro 600 Stunden Bildmaterial von versteckten Kameras aus einem Betrieb in Oldenburg aus, das dem Verein von anonymen TierschützerInnen zugespielt wurde. Es zeigt unter anderem ausblutende Rinder, die vor der Schlachtung nicht fachgerecht betäubt wurden, und andere Tierquälereien. Öffentlichkeit und Behörden wurden vom Tierschutzbüro über dessen erste Eindrücke im November vom Tierschutzbüro-Vorsitzenden Jan Peifer informiert: „Da kommt noch was.“

Versteckte Kameras haben sich zum wirksamsten Instrument der Tierschutzlobby in ihrem Kampf gegen Massentierhaltung und Schlachtindustrie entwickelt. Regelmäßig veröffentlichen Organisationen Aufnahmen, die das Grauen im Umgang mit den sogenannten Nutztieren zeigen. Der Betreiber eines ökozertifizierten Hofs in Brandenburg hat nach einer solchen Veröffentlichung das Schlachten vorerst eingestellt. In Niedersachsen, dem produktivsten deutschen Agrarbundesland, musste zuletzt ein Betrieb in Bad Iburg nach Videoenthüllungen schließen. Jetzt beschäftigen die Aufnahmen aus Oldenburg Behörden, Lebensmittelwirtschaft und Verbraucherschaft. Bestärkt fühlen sich die Undercover-AktivistInnen durch ein Urteil des Bundesgerichtshofs vom Frühjahr 2018, wonach Fernsehsender auch illegal aufgenommene Filme zeigen dürfen, wenn diese Wahrheiten von öffentlichem Interesse zeigen.

Der Europäische Tierärzteverband fordert schon seit langem die staatliche Videoüberwachung von Schlachthöfen. Susanne Mittag, Tierschutzbeauftragte der SPD, wies im Mai 2018 darauf hin, dass solche Kameras laut Rechtsgutachten des Wissenschaftlichen Dienstes des Bundestages möglich wären. Großbritannien hat sie schon, Frankreich testet noch. Aus dem Bundeslandwirtschaftsministerium, das die Kamerapflicht einführen müsste, gab es bisher nicht viel Sympathie für die Idee. Das Haus von Ressortchefin Julia Klöckner (CDU) äußerte arbeits- und datenschutzrechtliche Bedenken. Auch Barbara Otte-Kinast aus Niedersachsen dämpfte die Erwartungen. Eine Videoüberwachung könne nur eine unvollständige Ergänzung zu den Stichprobenkontrollen der lokalen Veterinärämter sein: „Eine lückenlose Rund-um-die-Uhr-Überwachung aller tierschutzrelevanten Betriebsbereiche ist von den zuständigen Veterinärbehörden nicht zu leisten.“ Deshalb hält auch Jan Peifer vom Tierschutzbüro die Idee für fragwürdig: „Wer soll die Bilder anschauen?“ Mit all der Arbeit, die sein Verein mit den Schlachthof-Filmen aus Oldenburg hatte, meinte er aber: „Die können gerne uns anstellen“ (Hahn, Kamera läuft, SZ 12.11.2018, 1).

Nordrhein-Westfalen

Neue Befugnisse im Polizeigesetz verabschiedet

Mit breiter Mehrheit hat sich der nordrhein-westfälische Landtag am 12.12.2018 dafür ausgesprochen, die Befugnisse der Polizei zu erweitern mit dem Argument, den Kampf gegen den Terrorismus zu erleichtern. Für die lange umstrittene Reform des Polizeigesetzes stimmte neben der aus CDU und FDP bestehenden Koalition auch die SPD, nachdem Schwarz-Gelb noch einige Korrekturen zugesagt hatte. Nur die Grünen lehnten die Initiative ab, mit der die Polizei auch außerhalb von Strafverfahren künftig etwa mit richterlicher Erlaubnis per Staatstrojaner Internet-Telefonate überwachen und Nachrichten von Messenger-Diensten wie WhatsApp auslesen dürfen. Die AfD enthielt sich (vgl. DANA 1/2018, 27-29).

Während die Regierung der Polizei auch eine Lizenz für heimliche Online-Durchsuchungen geben wollte, hat die Koalition im Landtag diese mit einem Änderungsantrag auf das Abgreifen „laufender“ Telekommunikation beschränkt. Die Maßnahme ist zulässig zur Abwehr einer „gegenwärtigen Gefahr“ für den Bestand oder die Sicherheit des Bundes oder eines Landes sowie für Leib oder Leben einer Person. Auch wenn der Polizei konkrete Anzeichen vorliegen, dass jemand „innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat“ begehen wird, kann sie den Staatstrojaner in Position bringen. Die ursprüngliche Planung, ebenso wie in Bayern als neuen Rechtsbegriff die „drohende Gefahr“ ins Gesetz aufzunehmen, wurde aufgegeben. Stattdessen werden nun konkrete schwere Straftaten aufgezählt, die drohen müssen, ehe eine Person präventiv – also ohne begangenes Vergehen – z. B. in „Unterbindungsgewahrsam“ genommen werden kann.

Mit der Quellen-Telekommunikationsüberwachung soll es möglich werden, auch auf kryptografisch geschützte

Kommunikation vor einer Ver- oder nach einer Entschlüsselung direkt auf Endgeräten der Zielperson zuzugreifen. Eingeschlossen sind Übermittler von Mitteilungen für einen Verdächtigen oder Personen, die diesem ihre Anschlüsse, Smartphones oder Rechner zur Verfügung stellen. Berufsgeheimnisträger wie Geistliche, Abgeordnete, Ärzte oder Rechtsanwälte bleiben außen vor.

Die Polizei darf terroristische Gefährder zudem künftig mit elektronischen Fußfesseln überwachen. In bestimmten Fällen kann das Tragen eines solchen Ortungsinstruments auch bei Sexualstraftätern, Stalkern oder in schweren Fällen häuslicher Gewalt angeordnet werden. Die Videoüberwachung wird ausgeweitet: Bisher durften Kameras nur an öffentlichen Plätzen angebracht werden, an denen bereits Verbrechen stattgefunden haben. Künftig reichen Anhaltspunkte aus, „dass dort Straftaten von erheblicher Bedeutung verabredet, vorbereitet oder begangen werden".

Zulässig wird ferner eine „strategische Fahndung" ohne konkreten Verdacht. Ordnungshüter dürfen Menschen so anhalten und nach ihrem Ausweis fragen oder sich Taschen beziehungsweise den Kofferraum eines Autos zeigen lassen, wenn ein Anlass wie eine Einbruchserie in einer Gegend besteht. Wer sich weigert, seine Identität feststellen zu lassen, kann statt zwölf Stunden fortan sieben Tage festgehalten werden. Maximal darf die Polizei Gefährder mit Verlängerung vier Wochen in Gewahrsam nehmen. Bisher liegt die Grenze hier bei 48 Stunden. Bis Ende 2022 soll die Regierung das Gesetz evaluieren lassen.

Bei einer parlamentarischen Anhörung hatten ExpertInnen im Vorfeld unter anderem verfassungsrechtliche Bedenken gegen die Initiative vorgebracht. Tausende DemonstrantInnen protestierten gegen den Entwurf auf der Straße. Die Grüne Verena Schäffer beklagte bei der abschließenden Lesung, der „grottenschlechte" Entwurf bringe tiefe Eingriffe in die Grundrechte mit sich. Die Regierung habe Ängste in der Bevölkerung geschürt, obwohl die Zahlen in der Kriminalstatistik von NRW rückläufig seien. Der Staat dürfe sich nicht zum Hacker machen. Außerdem kritisierten die Grünen, dass nach dem neuen Gesetz DemonstrantInnen, die sich etwa bei Protesten im Hambacher Forst einer Identitätsfeststellung verweigern, künftig sieben Tage lang festgehalten werden dürfen. Ein FDP-Abgeordneter warf den Grünen deshalb „Klientelpolitik" zum Schutze von Straftätern vor. Die Grünen-Fraktion prüft, ob sie eine Verfassungsbeschwerde gegen das Gesetz einlegen will. In Ländern wie Baden-Württemberg oder Hessen hatten die Grünen der Einführung von Staatstrojanern im Polizeirecht zugestimmt.

Marc Lürbke unterstrich im Namen der FDP-Fraktion, dass die Sicherheit im Land verbessert werde, Bürgerrechte aber gewahrt blieben. Hartmut Ganzke (SPD) lobte, dass das ursprüngliche Papier in intensiven Verhandlungen entschärft worden sei. Innenminister Herbert Reul (CDU) wertete einen tags zuvor erfolgten Anschlag in Straßburg als Zeichen, dass die Terrorgefahr real sei. Mit den beschlossenen Maßnahmen könne die Polizei endlich gegen terroristische Gefährder vorgehen, „bevor die Bombe explodiert ist". Das Sicherheitsgesetz sei in erster Linie ein Anti-Terror-Paket, ziele aber etwa auch auf Hooligans oder Pädophile ab (Krempl, Neues Polizeigesetz beschlossen: Der NRW-Trojaner kommt, www.heise.de 13.12.2018, Kurzlink: https://heise.de/-4250283; Gesetz gegen Gefährder, SZ 31.12.2018, 6).

Sachsen-Anhalt

Neuer Datenschutzbeauftragter wohl erst nach Verfassungsänderung

Nach drei gescheiterten Wahlgängen im Landtag für einen Beauftragten für den Datenschutz soll in Sachsen-Anhalt nun eine Verfassungsänderung helfen. Sachsen-Anhalt ist weiterhin auf der Suche nach einem neuen Landesbeauftragten als Nachfolge für Harald von Bose. Nils Leopold (Grüne), Kandidat der schwarz-rot-grünen Koalition, hatte bei einer dramatischen Landtagssitzung im Mai 2018 in drei Wahlgängen die nötige Mehrheit von zwei Dritteln der Parlamentarier verfehlt (vgl. DANA 2/2018, 101, 108 f.). Diskutiert wird nun eine Verfassungsänderung, um die hohe Hürde der Zwei-Drittel-Mehrheit aus dem Weg zu räumen. Ministerpräsident Reiner Haseloff sagte, die Verantwortung liege beim Landtag: „Ich habe einen Vorschlag gemacht." Er gehe davon aus, dass der Erkenntnisprozess im Parlament weiterlaufe. Er betonte, die Behörde sei funktionsfähig. Von Bose sei bereit, dort weiter zu arbeiten: „Darüber bin ich sehr froh".

Grünen-Fraktionschefin Cornelia Lüddemann kritisierte dagegen, Haseloff mache es sich zu einfach. Leopold war auf Initiative der Grünen vorgeschlagen worden. Haseloff habe sich den Vorschlag zu eigen gemacht und für Leopold geworben. Jetzt zu sagen, der Landtag sei am Zug, greife zu kurz: „Wir als Grüne warten auf ein belastbares Signal der Koalitionspartner und des Ministerpräsidenten." Leopold hat inzwischen klar gemacht, dass er nicht mehr zur Verfügung steht. Die Fraktionen von CDU und SPD setzen auf eine Änderung der Landesverfassung, um die Hürde der Zwei-Drittel-Mehrheit zu senken. Einen anderen Vorschlag gebe es bislang nicht, sagte SPD-Sprecher Martin Krems-Möbbeck. CDU, SPD und Grüne haben in ihrem Koalitionsvertrag wegen anderer Punkte ohnehin eine Verfassungsänderung vereinbart – so soll etwa ein Verbot der Diskriminierung aufgrund der sexuellen Identität aufgenommen werden. In diesem Zusammenhang könne man auch das Quorum für die Wahl des Datenschutzbeauftragten senken.

Auch Grünen-Fraktionschefin Lüddemann zeigte sich offen für eine Verfassungsänderung. Es sei unverständlich, dass die Hürde zur Wahl des Datenschutzbeauftragten höher sei als etwa für die Wahl des Ministerpräsidenten. Die geplante Änderung, auch zu anderen Punkten, sei aber ein aufwändiges Projekt. Sie hoffe, dass bis zur Sommerpause ein abstimmungsfertiges Paket vorliege. Gleichzeitig mahnte Lüddemann, eine Verfassungsänderung werde das Problem nicht lösen, wenn gleichzeitig eine Gesamtstrategie in Sachen Datenschutz fehle. Wie brisant das Thema sei, habe sich gerade wieder durch den Online-Angriff auf Daten von Politikern und Prominenten gezeigt (Ribnitzky, Sachsen-Anhalt weiter ohne neuen Datenschützer: Ausweg Verfassungsänderung? www.heise.de 14.01.2019, Kurzlink: https://heise.de/-4273037).

Datenschutznachrichten aus dem Ausland

Weltweit

Riesenhack bei Mariott/ Starwood

Eine wichtige Reservierungsdatenbank des Hotelkonzerns Marriot International wurde gehackt. In der Datenbank fanden sich Informationen zu rund einer halben Milliarde KundInnen. Gemäß Geschäftsführer Arne Sorenson ging es um Reservierungen, die vor dem 10.09.2018 in bestimmten Hotels der Kette getätigt wurden: „Wir bedauern diesen Vorfall zutiefst." Das Unternehmen machte das Datenleck am 30.11.2018 selbst auf seiner Webseite bekannt. Die Aufsichtsbehörden seien eingeschaltet worden. Ziel der Attacke war demnach die Reservierungsdatenbank der Marriott-Tochter Starwood. Darin werden Gästeinformationen gespeichert, die zu Tochtermarken wie zum Beispiel Le Méridien, Sheraton Hotels & Resorts und Westin Hotels & Resorts gehören. Marriott selbst verwende ein separates Reservierungssystem, das sich in einem anderen Netzwerk befinde.

Gemäß Unternehmensangaben gab es bereits seit 2014 „unbefugten Zugang" zum Starwood-Netzwerk. Eine eigene Untersuchung habe jetzt ergeben, dass jemand Unbekanntes Informationen aus dem System kopiert und verschlüsselt hat. Dem zufolge wurden im Laufe der Zeit Informationen kopiert, die über Gäste der Hotels gespeichert worden waren. Insgesamt sind demnach bis zu 500 Millionen Gäste betroffen. Zu 327 Millionen davon enthielt die Datenbank allerlei persönliche Daten, darunter „Namen, Postanschriften, Telefonnummern, E-Mail-Adressen, Passnummern, ‚Starwood Preferred Guest'-Kontoinformationen, Geburtsdaten, Geschlecht, Ankunfts- und Abfahrtsdaten, Reservierungsdaten und Kommunikationspräferenzen". Zu den restlichen Gästen sollen weniger Informationen abrufbar gewesen sein. Die genaue Kombination der Daten variiere je nach Gast. Bei einer nicht näher genannten Zahl an Personen hätten auch Zahlungskartennummern und Karten-Ablaufdaten zu den kopierten Informationen gehört. Die Zahlungskartennummern seien verschlüsselt gewesen: „Für die Entschlüsselung der Zahlungskartennummern sind zwei Komponenten erforderlich, und Marriott konnte an dieser Stelle nicht ausschließen, dass beides entnommen wurde."

Gemäß eigenen Angaben betreibt Marriott in 129 Ländern und Regionen Hotels. Die Firma aus dem amerikanischen Bethesda im US-Bundesstaat Maryland zählt damit zu den größten Hotelunternehmen der Welt. Starwood wurde von dem Konzern im Jahr 2016 übernommen, also zu Zeiten, als der Zugriff auf die Reservierungsdatenbank bereits begonnen hatte. Potenziell betroffene KundInnen sollten, so Mariott, sicherheitshalber auf ihren Kontoauszügen für Zahlungskarten nach verdächtigen Aktivitäten Ausschau halten und dies gegebenenfalls sofort dem jeweiligen Kartenanbieter melden. Zudem: „Marriott wird Sie nicht auffordern, Ihr Passwort per Telefon oder E-Mail anzugeben". Das Unternehmen kündigte an, die betroffenen KundInnen auch per E-Mail zu informieren. Erhält also jemand eine E-Mail rund um den Marriott-Hack oder sonst eine unverlangte, verdächtige Mail, so sollte die Person vorsichtig sein. Hinter der Nachricht könnten Kriminelle stecken, die durch das Datenleck an die persönlichen Daten gelangt sind (Böhm, Hotelkette Marriott meldet massives Datenleck, www.spiegel.de 30.11.2018).

EU

Rat will verbesserte grenzüberschreitende Internetermittlungen

Der Rat der EU setzt sich mit knapper Mehrheit für konkrete Vorschläge zu einer „E-Evidence-Verordnung" (Verordnung über die Herausgabe elektronischer Beweismittel) ein, wonach europäische Polizei- und Justizbehörden bei Diensteanbietern elektronische Beweismittel anfordern könnten. Die Justizminister der EU-Länder unterstützten am 07.12.2018 einen Verordnungsentwurf der EU-Kommission, mit dem die Strafverfolgungsbehörden der Mitgliedsstaaten letztlich weltweit auf elektronische Beweismittel zugreifen dürften. Dies bezieht sich vor allem auf Daten, die in der Cloud gespeichert sind, sowie auf Meta- und Inhaltsdaten aus der elektronischen Kommunikation, etwa über E-Mail, SMS oder Whatsapp. Bei Straftaten, die mit Haft von mindestens drei Jahren bedroht sind, sollen sich Strafverfolger direkt an Provider oder Dienstanbieter in einem anderen Mitgliedstaat wenden können. Der Staat, in dem sich die betroffene Person befindet, soll praktisch kein durchgreifendes Mitspracherecht haben. An einigen Punkten will der EU-Rat den Entwurf noch verschärfen. So schlägt er etwa vor, einen Artikel zu nationalen Möglichkeiten für den Widerspruch gegen eine „Vorlageanordnung" beispielsweise zum Schutz von Grundrechten komplett zu streichen und durch ein weniger striktes „Notifizierungssystem" für bestimmte Datenkategorien zu ersetzen.

Firmen, die die geplanten Datenzugriffe prinzipiell verweigern, sollen gemäß dem EU-Rat mit Bußgeldern in Höhe von bis zu zwei Prozent des globalen Jahresumsatzes sanktioniert werden können. Dies könnte für Internetgrößen wie Amazon, Apple, Facebook oder Google auf Milliardenstrafen hinauslaufen. Bei Verstößen gegen die geplanten Vorschriften zum Löschen terroristischer Inhalte sind sogar Bußgelder in einer Höhe von bis zu vier Prozent des Konzernumsatzes vorgesehen.

Nach Meinung der Justizminister sollen bestehende nationale Schutzrechte wie die Presse- oder Meinungsfreiheit sowie für „fundamentale Interessen" in den beteiligten Ländern bei Antragstellung stärker beachtet werden. Gelten sollen die Regeln zudem erst nach einer Übergangsfrist

von 24 statt, so der Kommissionsvorschlag, sechs Monaten. Von dem Vorschlag werden Bestandsdaten wie Name und Anschrift oder Zugangskennungen und Passwörter sowie E-Mails, SMS und Chatnachrichten erfasst. Inhaltsdaten einschließlich Fotos oder Videos in der Cloud sind ebenfalls mit eingeschlossen, wenn sie der Verfolgung schwerer Straftaten dienen sollen und ein Gericht einen Antrag darauf genehmigt hat.

Justizbehörden aus einem Mitgliedstaat soll es gestattet werden, E-Beweismittel unabhängig vom Standort der jeweiligen Daten unmittelbar bei Diensteanbietern anzufordern, die in der EU tätig sind. Betroffene Provider müssten dann innerhalb von zehn Tagen auf einen Antrag antworten. In Notfällen soll die Frist auf sechs Stunden verkürzt werden können. Mit einer Anordnung ist auch eine Vorgabe zur Vorratsdatenspeicherung verknüpfbar.

Staaten wie Deutschland, Finnland, Lettland, die Niederlande oder Ungarn stellten sich gegen die mehrheitliche Ratsposition. Bundesjustizministerin Katarina Barley betonte, dass der beschlossene Text nicht zustimmungsfähig sei, weil der Grundrechtsschutz unzureichend bleibe. Die Verordnung könnte dazu führen, dass z. B. in Deutschland wegen Straftaten ermittelt werden könnte, die hier gar nicht strafbar sind. Sie hoffe nun auf Verbesserungen in den anstehenden Verhandlungen mit dem EU-Parlament, das seine Linie zu dem Dossier noch abstecken muss. Zuvor hatte die SPD-Politikerin mit Amtskollegen aus sieben weiteren Ländern in einem Brief an die Kommission unter anderem auf eine behördliche Widerspruchsmöglichkeit in begründeten Fällen gedrängt. Dies sieht die Bundesrechtsanwaltskammer ähnlich, die in ihrer Stellungnahme darauf hinwies, dass so Deutschland verpflichtet würde zur „politisch motivierten Verfolgung wegen zu diesem Zweck geschaffenen Delikten“. Andere Kritiker verweisen auf Polen, wo Abtreibung verboten ist. Die Zustimmung eines Richters aus dem Ermittlerstaat gilt aus deutscher Sicht nicht als gleichwertiger Ersatz. Die deutsche Europaabgeordnete Birgit Sippel (SPD) sagte, sie teile viele der Bedenken, die gegen die E-Evidence-Verordnung vorgebracht werden: „Wir sind nicht gegen die Idee als solche. Aber unser Eindruck ist, dass hier sehr schnell über Bedenken hinweg gegangen wurde.“

Strafverfolger begrüßen die Initiative, so z. B. Oberstaatsanwalt Markus Hartmann, der in Köln eine Zentral- und Ansprechstelle für Cybercrime leitet: „Der Vorschlag ist die richtige Reaktion auf die Notwendigkeiten der Praxis. Wir haben im Bereich der Cyberkriminalität kaum ein Verfahren, das keine internationale Bezüge aufweist.“ Auch bei analogeren Straftaten wie Betrug und Erpressung steige die Bedeutung elektronischer Spuren. Dies zeige die Masse der Anfragen, die sein Team dazu erreiche. Will die Polizei oder die Staatsanwaltschaft auf Daten zugreifen, die in einem anderen Mitgliedstaat gespeichert sind, muss sie bislang den Weg der Rechtshilfe gehen, sich also an die Behörden des jeweiligen Staates wenden, die dann wiederum beim jeweiligen Provider um die Daten bitten. Hartmann: „Die traditionellen Mittel der Rechtshilfe dauern zu lange.“

Die Datenschutzbeauftragten des Bundes und der Länder meinen, Grundrechte der Nutzenden und der Provider würden mit der geplanten E-Evidence-Verordnung mit Füßen getreten und Schutzvorschriften zur Vorratsdatenspeicherung ausgehebelt. Sie befürchten laut einer Entschließung, dass Drittstaaten die Verordnung als Blaupause für vergleichbare Auflagen heranziehen werden. Der Entwurf enthalte so viele Mängel, dass ihn die am Gesetzgebungsverfahren beteiligten Gremien stoppen müssten. Der Digitalverband Bitkom begrüßte zwar prinzipiell, dass die E-Evidence-Verordnung die grenzüberschreitende Strafverfolgung beschleunigen könnte. Die Fristen für eine Datenherausgabe seien aber viel zu kurz bemessen, um etwaige Behördenanfragen inhaltlich korrekt zu prüfen. (Krempl, E-Evidence: EU-Staaten befürworten breiten Zugriff auf Cloud-Daten, www.heise.de 07.12.2018, Kurzlink: https://heise.de/-4245414; Beisel, Schnelles Netz für die Rechtshilfe, SZ 06.12.2018, 6; Rath, Fahnder erhalten Zugriff auf E-Mails, SMS und Whatsapp, Kieler Nachrichten 08.12.2018, 5).

EU

Datenmissbrauch im Wahlkampf soll sanktionierbar sein

Die EU will den demokratischen Prozess besser vor Desinformationskampagnen schützen, für die Daten von WählerInnen missbraucht werden. Deshalb gelten künftig für politische Gruppierungen in der EU strengere Regeln. Eine Partei oder eine ihr nahestehende Stiftung soll mit Geldstrafen belegt werden, wenn sie im Wahlkampf gegen Datenschutzbestimmungen verstößt. Auf einen entsprechenden Verordnungsentwurf haben sich am 16.01.2019 die Mitgliedsstaaten, das EU-Parlament und die Kommission in Straßburg geeinigt. Betroffene Institutionen sollen eine Strafe in Höhe von bis zu fünf Prozent ihres Jahresbudgets zahlen müssen. Damit reagieren die EU-Gremien v. a. auf den Datenskandal um Cambridge Analytica. Die britische Big-Data-Firma hatte sich während des US-Wahlkampfs unerlaubt Zugang zu Daten von Millionen Facebook-Nutzenden verschafft. Mit den Informationen soll Cambridge Analytica über Beiträge und Werbung in dem sozialen Netzwerk geholfen haben, für den heutigen US-Präsidenten Donald Trump zu mobilisieren und zugleich potenzielle WählerInnen der Gegenkandidaten Hillary Clinton vom Urnengang abzuhalten.

Um derlei Desinformationskampagnen zu erschweren, wird es politische Kräfte fortan teurer zu stehen kommen, wenn sie bewusst Datenschutzverletzungen in Kauf nehmen, um das Ergebnis europäischer Wahlen zu beeinflussen – oder es versuchen. In der Praxis sollen nationale Aufsichtsämter entscheiden, ob etwa eine Partei gegen diese neuen Vorgaben verstoßen hat. Danach muss die 2014 eingerichtete Behörde für europäische politische Parteien und Stiftungen die Resultate der Ermittlungen überprüfen und gegebenenfalls die geforderte Sanktion verhängen. Im März 2019 sollen die verschärften Bestimmungen dann direkt nach der Veröffentlichung im EU-Amtsblatt in Kraft treten. Damit könnten sie in allen Mitgliedsstaaten noch vor den europäischen Wahlen greifen, die zwischen dem 23. und dem 26. Mai 2019 durchgeführt werden.

Der Vorschlag ist Teil eines größeren Maßnahmenpakets gegen Wahlmanipulationen. Darin sind u. a. Impressumspflichten für Wahlwerbeinhalte und weitergehende Transparenz-, Fairness- und Stillhaltepflichten für Online-Kampagnen vorgesehen. Auch ein Verbot, Profile über WählerInnen anzulegen, sowie eine Kennzeichnungspflicht für den massenhaften Einsatz von Social Bots sind danach vorgesehen (Krempl, EU: Datenschutzverstöße durch Parteien im Wahlkampf werden sanktioniert, www.heise.de 17.01.2019, Kurzlink: https://heise.de/-4281080).

EU

Mit „künstlicher Intelligenz" gegen illegale Grenzübertritte?

Die Europäische Union (EU) testet seit November 2018 ein System „iBorderCtrl" an vier Grenzübergängen in Griechenland, Lettland und Ungarn, mit dem per „künstlicher Intelligenz" (KI) LügnerInnen an der Einreise gehindert werden sollen. Nach den Planungen der EU-Kommission könnten irgendwann alle Nicht-EU-BürgerInnen vor einem Grenzübertritt in die EU vor einer Kamera automatisiert befragt werden; ein mit KI arbeitender Lügendetektor würde dann die Antworten auf ihren Wahrheitsgehalt prüfen. Mit 4,5 Mio. € fördert Brüssel das auf sechs Monate begrenzte Pilotprojekt aus Luxemburg, an dem Forschende aus acht Staaten beteiligt sind. Das Verfahren hat zwei Stufen: Zu Hause lädt der Reisende zunächst Dokumente wie Pass, Visum, Foto oder Einkommensnachweis hoch. Auf dem Bildschirm erscheint eine virtuelle GrenzbeamtIn in blauer Uniform, deren Geschlecht, Ethnizität und Sprache an die sich bewerbende Person angepasst sind.

Während der Avatar mehr über Kofferinhalt und den geplanten Aufenthalt in der EU wissen will, zeichnet die Kamera alles auf und eine Software analysiert die kleinsten Regungen im Gesicht, die die Bewerbenden nicht kontrollieren können. Anhand von 38 dieser Mikroimpressionen sollen Personen überführt werden, die lügen. Das System teilt die KandidatInnen in Kategorien ein: Wer als „bedrohlich" eingestuft wird, müsste in der zweiten Stufe am Grenzposten genauer geprüft werden. Dabei soll den BeamtInnen ein mobiler Scanner helfen, der die gesammelten biometrischen Daten mit den EU-Datenbanken abgleichen soll. Dank Radar könnte er auch nebenbei Menschen erkennen, die sich in Hohlräumen verstecken. Aus ihren Zielen macht die EU-Kommission kein Geheimnis: Kontrollen sollen schneller und illegale EinwandererInnen besser erkannt werden. Für den Kriminologen Bennett Kleinberg vom University College London ist der Ansatz „pseudowissenschaftlich" und problematisch: „Es ist sehr umstritten, dass es eine Beziehung von nonverbalen Mikroimpressionen wie dem Zucken eines Augenlids und dem Erzählen einer Lüge gibt." Stress sei kein guter Indikator für die Wahrheitsfindung.

Der Lügendetektor wurde bisher nur an 32 Menschen getestet und hat dabei eine Erfolgsquote von 76% erzielt. Die Expertin Maja Pantić wies darauf hin, dass die Hälfte der Teilnehmenden bewusst geflunkert habe, weshalb die Software mit fehlerhaften Daten gefüttert werden könnte: „Wenn man Leute bittet, nicht die Wahrheit zu erzählen, verhalten sie sich anders als jemand, der wirklich lügt, um nicht ins Gefängnis zu müssen." Keeley Crockett von der Manchester Metropolitan University, die „iBorderCtrl" berät, erklärte, dass diese Herausforderungen bekannt seien. Sie betont, dass das System nicht allein entscheiden würde, sondern GrenzbeamtInnen unterstützen soll. Crockett hofft, dass sich die Erfolgsquote durch den Pilotversuch auf 85 Prozent erhöht. Bei mehr als 700 Millionen Menschen, die jährlich in die EU einreisen, würde dies immer noch zu einer riesigen Zahl an Fehldiagnosen führen. In der Pilotphase werden nur Freiwillige aufgezeichnet (Kolb, Schau mir in die Augen, SZ 05.11.2018, 1).

Österreich

Post verkauft Daten zu politischer Affinität

Im Rahmen seines seit Jahren betriebenen Datenhandels bietet die Österreichische Post Werbetreibenden Informationen über drei Millionen ÖsterreicherInnen feil. Zu den Daten gehört etwa, ob die Betroffenen gerne laufen, wie alt sie sind, ihre Familiensituation, oder wie häufig sie Pakete bekommen. Für 2,2 Millionen Personen wird auch eine Bewertung der „Affinität" zu bestimmten politischen Parteien verkauft. Das ist juristisch bedenklich.

Die Datenschützer von epicenter.works halten diese Geschäfte der Post für illegal. Art. 9 der EU-Datenschutzgrundverordnung (DSGVO) verbietet ausdrücklich die Verarbeitung personenbezogener Daten, aus denen politische Meinungen hervorgehen – außer, der Betroffene hat ausdrücklich für bestimmte Zwecke zugestimmt, was nur sehr selten gegeben sein dürfte. Die Österreichische Post verteidigt ihr Geschäftsmodell und hält es mit folgender Begründung für legal: Die angepriesenen Daten über die Parteiaffinitäten seien nicht unbedingt „tatsächlich zutreffend". Tatsächlich handle es sich nicht um konkretes Wissen, sondern um Ableitungen aus Geschlecht und Alter sowie statistischen Daten wie regionaler Kaufkraft und Durchschnittseinkommen, Wahlergebnissen, Einkommen und repräsentativen Umfragen. Die Post verglich ihr Angebot mit Hochrechnungen am Wahlabend.

Tatsächlich dürften die Daten über die Parteiaffinität nur geringe Aussagekraft haben. 30 ÖsterreicherInnen haben ihr Recht auf Selbstauskunft gegenüber der Post geltend gemacht und die erhaltenen Antworten für eine Auswertung zur Verfügung gestellt. Bei weniger als der Hälfte der Stichprobe hatte die Post die Parteiaffinität richtig bestimmt. Dies macht die Vorgehensweise der Österreichischen Post aber noch fragwürdiger: Die falsche Andichtung der Affinität zu einer bestimmten politischen Partei könnte nicht nur ein Datenschutzverstoß, sondern auch ein weitergehender Eingriff in die Persönlichkeitsrechte des Betroffenen sein.

Im Übrigen betont die Österreichische Post, die Daten nur für Marketingzwecke zu verkaufen. Setzt ein Kunde die Daten dennoch anders ein, verstoße er gegen den Vertrag mit seinem Datenhändler. Zu diesen Kunden zählen andere Datenhändler, darunter auch solche

in Deutschland, Unternehmen wie zum Beispiel Stromanbieter oder schwedische Möbelhäuser, und natürlich politische Parteien in Österreich. Die liberale Partei NEOS hatte 2015 Strafe zahlen müssen, nachdem sie bei der Post die Handynummern zahlreicher BürgerInnen in Wien gekauft, und dann an diese SMS geschickt hatte. Der Datenkauf war legal, das Spammen nicht.

Ähnliches gilt für die Post: Daten sammeln darf sie, weil sie einen Gewerbeschein für Adresshandel gelöst hat. Feilbieten darf sie die Daten aber nur mit Zustimmung der Betroffenen. Und diese holt sich die Post gerne im Kleingedruckten bei Anmeldungen für Mailinglisten, Teilnahmen an Gewinnspielen, und, besonders ausgefuchst, bei Nachsendeanträgen. 2001 wurde die Post für ihren Datenhandel mit einem österreichischen Big Brother Award bedacht, 2008 erhielt sie sogar den speziellen „Ehrenpreis für das lebenslange Ärgernis".

Auch die deutsche Post hatte über eine Tochter im Bundestagswahlkampf 2017 Adressdaten an CDU und FDP verkauft. Dabei seien aber nur anonymisierte Daten genutzt worden, beteuerten die Parteien. Die Post erklärte, nur statistische Wahrscheinlichkeitswerte dargestellt zu haben: Die Daten bezögen sich somit nicht auf einzelne Haushalte (Sokolov, Datenhandel: Österreichische Post verkauft Partei-Affinität der Österreicher, www.heise.de 08.01.2019, Kurzlink: https://heise.de/-4267637).

Österreich

Verfassungsgerichtshof stoppt Staatsbürgerschaftsentzug über dubiose Liste

Der Verfassungsgerichtshof Österreichs stoppte im Dezember 2018 die Nutzung einer Liste mit mehr als 100.000 Namen von Austro-TürkInnen, die der rechtspopulistischen Regierungspartei FPÖ nach eigenen Angaben im Frühjahr 2017 „zugespielt" worden war, durch die Staatsangehörigkeitsbehörden. Viele ÖsterreicherInnen mit türkischen Wurzeln hatten zuvor in Unsicherheit und mit der Angst gelebt, unter dem Vorwurf der illegalen Doppel-Staatsbürgerschaft ihren österreichischen Pass zu verlieren. Die Behörden hatten, befeuert durch die FPÖ, landesweit ermittelt. Die FPÖ will sich mit der höchstrichterlichen Entscheidung nicht zufriedengeben und legte mit dem Vorschlag ihres Parteichefs Heinz-Christian Strache nach, die Verleihung neuer österreichischer Staatsbürgerschaften an Menschen aus der Türkei vorerst generell auszusetzen.

Ausgangspunkt des ziemlich komplizierten Falls ist eine Liste, bei der es sich um eine „Wählerevidenzliste" der türkischen Behörden handeln soll. Von wem und aus welchen Motiven sie an die FPÖ weitergeleitet wurde, wurde nicht enthüllt. Für die Freiheitlichen ist diese Liste der Beweis dafür, dass sogenannte Austro-TürkInnen in großer Zahl ihr Wahlrecht in der Türkei ausüben, obwohl sie dort eigentlich nach österreichischem Recht gar keine StaatsbürgerInnen mehr sein dürften.

In Österreich sind Doppelstaatsbürgerschaften grundsätzlich verboten. Wer sich einbürgern lässt, muss den Pass seines Herkunftslandes abgeben. Ausnahmen gibt es für Kinder aus binationalen Ehen sowie für KünstlerInnen, SportlerInnen oder WissenschaftlerInnen, an denen Österreich ein gezieltes Interesse hat. Die FPÖ kämpft überdies noch für eine weitere Ausnahmeregelung für SüdtirolerInnen, denen ein Doppelpass im Koalitionsvertrag in Aussicht gestellt wurde. Dieser Pass soll aber nicht türkischen EinwandererInnen offen stehen, die seit jeher von den Rechtspopulisten verdächtigt werden, so Parteichef Strache, in „Parallel- und Gegengesellschaften" zu leben.

Das Thema wurde im Wahlkampf 2017 kräftig hochgespielt. Strache hatte die Behörden aufgefordert, noch vor der Abstimmung all jene aus den österreichischen Wählerlisten zu streichen, die sich illegalerweise den Pass ihres Ursprungslandes zurückgeholt hätten. So schnell konnte das zwar nicht gehen, aber landesweit wurden die Ämter nun anhand der von der FPÖ weitergeleiteten türkischen Liste aktiv. Allein in der Hauptstadt Wien, wo die weitaus größte Zahl türkischer Einwandernder lebt, wurden 18.000 sogenannte Feststellungsverfahren eingeleitet. Die zuständige Magistratsabteilung wurde dafür um 20 Mitarbeitende aufgestockt. Abgeschlossen wurden bisher landesweit mindestens 85 Verfahren, in denen Austro-TürkInnen ihren Pass verloren.

Nachdem Ende September 2018 der Verwaltungsgerichtshof die Verwendung der Liste als Beweismittel genehmigt hatte, wuchs die Unsicherheit bei all jenen, deren Name sich darauf fand. Der Verfassungsgerichtshof als höchste Instanz sorgte nun jedoch Ende 2018 für Klarheit anhand der Klage eines Mannes, der seit mehr als 40 Jahren in Österreich lebt und seit 1996 die Staatsbürgerschaft besitzt: Die von der FPÖ weitergegebene Liste, so urteilten die Richter, sei „kein taugliches Beweismittel". Es sei lediglich eine „Vermutung", dass es sich dabei tatsächlich um ein korrektes Wählerverzeichnis handele. Denn dieser Datensatz sei „nicht authentisch und hinsichtlich seiner Herkunft und des Zeitpunkts seiner Entstehung nicht zuordenbar". Die Richter stellten fest, dass die Beweislast, keinen türkischen Pass mehr zu besitzen, nicht bei den Betroffenen liegen könne.

Als Reaktion darauf wurden in Wien alle 18.000 Feststellungsverfahren gestoppt. Von den 34 Personen, die dort bereits rechtskräftig ausgebürgert wurden, sollen 18 ihre Pässe zurückbekommen. Bei den anderen 16, so heißt es, sei der Passentzug nicht allein aufgrund der angeblichen Wählerliste erfolgt. Aus den Bundesländern kamen uneinheitliche Signale. In Oberösterreich zum Beispiel, wo ein Minister der FPÖ zuständig ist, sah man im Spruch des Verfassungsgerichtshofs keine Auswirkungen auf bereits entschiedene Fälle. Kanzler Sebastian Kurz betonte nach dem höchstrichterlichen Urteil, dass seine Regierung eine „ganz klare" Linie habe: „Wir wollen, dass es keinen Missbrauch bei der Staatsbürgerschaft gibt. Doppelstaatsbürgerschaften sind nicht vorgesehen." Straches Forderung nach einem vorläufigen Stopp der Einbürgerungen wollte er sich nicht zu eigen machen. Er wies Innenminister Herbert Kickl an, nun das weitere Vorgehen in diesem verwickelten Fall zu prüfen. Kickl gehört zur FPÖ (Münch, Fehlpass Strache, SZ 22./23.12.2018, 9).

Frankreich

Millionenstrafe gegen Google

Die französische Datenschutzbehörde CNIL (Commission Nationale de l'Informatique et des Libertés, deutsch Nationale Kommission für Informatik und Freiheiten) hat gemäß einer Mitteilung vom 21.01.2019 gegen Google nach Beschwerden von Max Schrems von noyb (non of your business) und La Quadrature du Net eine Geldstrafe in Höhe von 50 Mio. € wegen Verstößen gegen die EU-Datenschutzgrundverordnung (DSGVO) verhängt. Unter anderem seien Informationen zur Verwendung der erhobenen Daten und dem Speicherzeitraum für die Nutzenden nicht einfach genug zugänglich. Sie seien über mehrere Dokumente verteilt und Nutzende müssten sich über mehrere Links und Buttons durchklicken. Zudem seien einige der Informationen unklar formuliert. Die von Google eingeholte Zustimmung zur Anzeige personalisierter Werbung sei unwirksam, weil die Nutzenden nicht ausreichend informiert würden. Die DSGVO sieht unter anderem vor, dass Unternehmen Nutzende transparent über die Verwendung ihrer Daten informieren müssen. Die CNIL erklärte die Höhe der Strafe mit der Schwere des Verstoßes, der die Grundprinzipien der DSGVO betreffe: Transparenz, Information und Zustimmung. Es handelt sich um die erste Strafe der Behörde nach der DSGVO. Gemäß der Verordnung können Strafen von bis zu vier Prozent des Jahresumsatzes eines Unternehmens verhängt werden.

Google teilte mit, das Unternehmen werde nach einer ausführlichen Prüfung des Beschlusses Widerspruch einlegen. Es zeigte sich über die Folgen der CNIL-Entscheidung für Inhalte-Autoren sowie IT-Unternehmen insgesamt „besorgt". Es habe hart an einem Zustimmungsverfahren für personalisierte Werbung gearbeitet, das möglichst transparent sein sollte und auf Empfehlungen der Regulierer basierte, erklärte der Internet-Konzern zur Begründung über sein weiteres Vorgehen in dem Fall. Google sei entschlossen, die hohen Erwartungen der NutzerInnen an Transparenz und Kontrolle über die Daten zu erfüllen. Für den Internet-Konzern ist die Strafe ein kleiner Betrag. So steckte Google die Wettbewerbsstrafen der EU-Kommission in Höhe von 4,34 Mrd. Euro vom Juli 2018 wegen der marktbeherrschenden Stellung beim Android-Betriebssystem locker weg. Zugleich klagt Google dagegen vor Gericht.

Google hatte inzwischen die bereits im Dezember 2018 angekündigte Einrichtung einer europäischen Hauptniederlassung in Irland vollzogen. Damit ist nun die irische Datenschutzbehörde für alle grenzüberschreitenden Fälle in Europa zuständig. Diese Bündelung bei einem Regulierer gehört zu den Neuerungen der DSGVO. Bei lokalen Einzelfällen mit Betroffenen in einem EU-Mitgliedsstaat sind weiterhin die Datenschützer des jeweiligen Landes zuständig. Bis zur Einrichtung der Hauptniederlassung konnten sie auch grenzübergreifend aktiv werden – wovon die CNIL Gebrauch machte (Google klagt gegen EU-Strafe, SZ 11.10.2018, 19; DSGVO-Verstöße: Frankreich verhängt Millionen-Strafe gegen Google, www.heise.de 21.01.2019, Kurzlink: https://heise.de/-4283765; Millionenstrafe für Google, SZ 22.01.2019, 22; Google geht in Berufung gegen französische Datenschutz-Strafe, www.heise.de 24.01.2019, Kurzlink: https://heise.de/-4286263).

Niederlande/Großbritannien

600.000 €-Strafe gegen Uber wegen Data-Breach-Verschweigen

Die niederländische Datenschutzbehörde hat eine Strafe von 600.000 € gegen den Fahrdienstvermittler Uber verhängt. Betroffen waren demnach auch 174.000 NiederländerInnen. In Großbritannien, wo es um 2,7 Millionen KundInnen und fast 82.000 FahrerInnen geht, soll Uber 385.000 Pfund (rund 434.000 Euro) zahlen. Das US-Unternehmen habe den immensen Diebstahl von 57 Millionen Nutzerdaten nicht innerhalb der vorgegebenen Frist von 72 Stunden nach der Entdeckung gemeldet. Abgegriffen worden waren Namen, E-Mail-Adressen und Telefonnummern von Uber-Nutzenden. Das massive Datenleck war im Dezember 2017 bekannt geworden, der Diebstahl hatte sich aber bereits 2016 ereignet und bei Uber war er damals auch bereits entdeckt worden (DANA 1/2018, 52). Der damals noch neue Uber-Chef Dara Khosrowshahi hatte das lange Schweigen nicht entschuldigen wollen und erklärt, „nichts davon hätte passieren dürfen". Der Konzern war dann noch einmal in die Kritik geraten, als bekannt wurde, dass der verantwortliche Hacker 100.000 US-Dollar aus dem hauseigenen Bug-Bounty-Programm bekommen hatte, damit er im Gegenzug die Daten löscht. Das Programm ist eigentlich als Anreiz gedacht, damit Sicherheitsforscher von ihnen entdeckte Software-Lücken direkt an Uber melden, statt anderswo Kapital daraus zu schlagen (Holland, Datenleck verschwiegen: 600.000 Euro Strafe in den Niederlanden gegen Uber, www.heise.de 27.11.2018, Kurzlink: https://heise.de/-4233285; Datenschutz-Strafen für Fahrdienst-Vermittler Uber, www.donaukurier.de 27.11.2018).

Italien

Wettbewerbsstrafe gegen Facebook

Die italienische Wettbewerbsbehörde AGCM hat gegen Facebook zwei Datenschutz-Strafen in Höhe von zusammen 10 Millionen Euro verhängt. Facebook wird vorgeworfen, Internetnutzende in die Irre zu führen, wenn es vor der Kontoeröffnung vor allem darauf hinweist, dass die Nutzung kostenlos ist. Dass Nutzerdaten für kommerzielle Zwecke gesammelt werden, sei dagegen nicht klar ersichtlich. Es sei zu befürchten, dass Nutzende sich anders entscheiden würden, wenn sie vor der Kontoeröffnung angemessen auf diese Aspekte hingewiesen würden.

Zudem kritisieren die Wettbewerbshüter die Weitergabe von Nutzerdaten bei der Anmeldung mit einem Facebook-Account bei anderen Websites und Apps. Sie werfen Facebook eine aggressive Geschäftspraxis vor, wenn Daten ohne ausdrückliche Zustimmung der Nutzenden an andere Plattformen weitergegeben werden. Die vorgesehenen Abwahl-Möglichkeiten für die Funkti-

on seien nicht ausreichend. Facebook müsse das ändern und prominent auf die Anpassungen hinweisen. Facebook erklärte am 07.12.2018, man prüfe die Entscheidung und hoffe, die Bedenken der Behörde ausräumen zu können. Zugleich versicherte das Unternehmen, dass Daten nicht ohne Zustimmung der Nutzenden mit anderen Apps oder Websites geteilt würden (Holland, Facebook: Zehn Millionen Euro Datenschutzstrafe in Italien, www.heise.de 07.12.2018, Kurzlink: https://heise.de/-4245630).

Großbritannien

Parlament beschafft sich geheime Unterlagen zum Facebook-Cambridge-Analytica-Skandal

Das britische Parlament hat in einem ungewöhnlichen Schritt die Herausgabe interner Facebook-Dokumente erzwungen. Darunter sollen sich auch E-Mails verantwortlicher Manager sowie von Facebook-Chef Mark Zuckerberg befinden. Der Vorsitzende des Digitalausschusses (Digital, Culture, Media and Sports Committee – DCMS), Damian Collins, nutzte gemäß Presseberichten einen nie zuvor angewandten parlamentarischen Prozess, um den Gründer der Softwarefirma Six4Three während einer Geschäftsreise nach London zur Herausgabe interner Facebook-Dokumente zu nötigen: Ein Sergeant-at-Arms habe ihn zunächst in seinem Hotel aufgesucht und ein Ultimatum von zwei Stunden gestellt, innerhalb dessen er die Dokumente zu übergeben habe. Nach Verstreichen dieser Frist wurde der Mann zum Parlament geleitet und dort informiert, dass Geld- und Gefängnisstrafe drohten, wenn er der Aufforderung nicht nachkäme.

Six4Three ist ein externer Facebook-Softwareentwickler, der juristisch gegen Facebook wegen der Investition in eine App vorgeht und den Social-Media-Konzern beschuldigt, von den fragwürdigen Implikationen seiner damals gültigen Privatsphären-Richtlinie gewusst zu haben, die Partnerfirmen wie Cambridge Analytica die nahezu uneingeschränkte Aneignung von Nutzerdaten (inklusive Freunden von Freunden ohne Einwilligung) erlaubt habe. Facebook soll zudem diese Situation gezielt herbeigeführt, für sich ausgenutzt und auf den praktisch ausgehebelten Datenschutz sogar hingewiesen haben. 2015 habe Facebook diese Situation zu bereinigen versucht und den Zugriff der Entwickler auf Nutzerdaten eingeschränkt. Einigen Entwicklern soll Facebook aber auch danach Zugriff auf Freunde-Daten gewährt haben. Facebook streitet diese Anschuldigungen ab und geht seinerseits juristisch dagegen vor.

In Zuge dieses Rechtsstreits zwischen Six4Three und Facebook hat ein US-amerikanisches Gericht in Kalifornien bereits verfügt, dass die fraglichen Dokumente in den USA nicht veröffentlicht werden dürfen. Facebook forderte nach der Beschlagnahme durch das britische Parlament das DCMS-Komitee auf, die Dokumente weder zu lesen noch zu veröffentlichen und sie zurückzugeben. Es ist fraglich, ob Collins dem nachkommen wird: „Dies ist ein beispielloser Vorgang, aber es ist auch eine beispiellose Situation. Wir haben von Facebook keine Antworten erhalten und wir glauben, dass diese Dokumente Informationen von hohem öffentlichen Interesse enthalten."

Die britische Datenschutzaufsicht hatte gegen Facebook wegen des Datenskandals bereits eine Strafe von 500.000 britischen Pfund verhängt. Der im März 2018 bekannt gewordene Skandal hatte bald darauf zur Einstellung der Geschäfte von Cambridge Analytica und seiner Muttergesellschaft geführt. Auch der Whistleblower Christopher Wylie, dessen Enthüllungen den Skandal ausgelöst hatten, bekräftigte, Facebook habe von Anfang an über die Situation Bescheid gewusst (Wittenhorst, Cambridge-Analytica-Skandal: Großbritannien beschlagnahmt Facebook-Dokumente, www.heise.de 25.11.2018, Kurzlink: https://heise.de/-4232212).

USA

Präsidenten-Tochter versendete offizielle Mails über Privataccount

Ivanka Trump, Tochter und ranghohe Beraterin von US-Präsident Donald Trump, hat Hunderte Dienstnachrichten von einem privaten E-Mail-Konto abgeschickt, die u. a. an Mitarbeitende im Weißen Haus, Mitglieder des Kabinetts und ihre AssistentInnen gerichtet waren. Derartige Mails müssen als offizielle Kommunikation von Gesetzes wegen amtlich archiviert werden. Die Mails wurden über eine Domain verschickt, die Trump gemeinsam mit ihrem Mann Jared Kushner eingerichtet hatte. Ein Anwalt von Ivanka Trump räumte die teilweise Nutzung des privaten Mail-Accounts seiner Mandantin ein und betonte, dies sei geschehen, bevor sie über die Regeln des Weißen Hauses zum Umgang mit E-Mails informiert worden sei. Er versicherte, keine dieser Mails habe als vertraulich eingestufte Informationen enthalten. Meist sei es um logistische Fragen und terminliche Absprachen mit der Familie gegangen: „Als vor 14 Monaten in der Presse Bedenken laut wurden, überprüfte und kontrollierte Frau Trump ihre E-Mail-Nutzung gemeinsam mit dem Rechtsbeistand im Weißen Haus und legte die Angelegenheit der Führung im Kongress dar." Die liberale Regulierungsorganisation American Oversight hatte den Vorgang aufgedeckt, so deren Exekutivdirektor: „Die Familie des Präsidenten steht nicht über dem Gesetz."

Dass Ivanka Trump nicht gewusst haben will, dass die Verwendung eines privaten E-Mail-Kontos nicht erlaubt ist, sorgte in Washington für einigen Spott angesichts der Tatsache, dass sie in der Wahlkampagne ihres Vaters eine wichtige Rolle gespielt hatte. Selbst Verbündete des Weißen Hauses sprachen davon, dass die Angelegenheit für den Präsidenten peinlich sei. Die E-Mail-Praxis seiner Tochter ist für den US-Präsidenten heikel, da er seiner Konkurrentin im Präsidentschaftswahlkampf 2016, Hillary Clinton, die Nutzung eines privaten Mail-Kontos für dienstliche Belange in höchst angriffslustiger Weise vorgehalten hatte. Unter anderem hatte er sie deshalb „betrügerische Hillary" genannt und erklärt, sie gehöre ins Gefängnis. Der Vorgang sei „schlimmer als Watergate". Trump hielt Clinton das Thema immer weiter vor und schlachtete die E-Mail-Affäre für seine Zwecke aus. Er twitterte darüber selbst zwei Jahre nach seinem Wahlsieg, und auch die „Sperrt sie ein"-Rufe seiner AnhängerInnen hört man bei Trumps Veranstal-

tungen noch heute. Clinton hatte in ihrer Zeit als US-Außenministerin offizielle E-Mails über einen privaten und nicht gesicherten Server verschickt. Sie ließ in ihrer Zeit als Außenministerin von 2009 bis 2013 ihre gesamte Korrespondenz über einen privaten E-Mail-Server in ihrem Privathaus im Bundesstaat New York laufen. Als dies 2015 bekannt wurde, verteidigte sich Clinton damit, sie habe zu keinem Zeitpunkt geheimes Material verschickt. Diese Behauptung wurde durch eine spätere Untersuchung des FBI widerlegt. Zudem ließ Clinton rund 30.000 E-Mails löschen mit der Begründung, diese seien rein privater Natur gewesen. Das FBI kam im Sommer 2016 zu dem Schluss, dass die Demokratin sich nicht strafbar gemacht habe (E-Mail-Affäre im Weißen Haus? www.tagesschau.de 20.11.2018; Cassidy, Erinnerungen an Hillary, SZ 21.11.2018).

USA

Gesichtserkennungs-Abgleich bei Taylor-Swift-Konzert

Bei einem Konzert der US-Sängerin Taylor Swift im Mai 2018 wurde einem Medienbericht zufolge heimlich eine Gesichtserkennung der BesucherInnen durchgeführt, um nach Personen zu suchen, die für Belästigungen der US-Sängerin bekannt waren. Demgemäß hat der Security-Experte Mike Downing nach eigener Aussage auf der Veranstaltung eine Vorführung des Systems begutachtet. Ihm zufolge war bei dem Konzert im kalifornischen Pasadena ein Bildschirm installiert, auf dem Videos der Proben gezeigt wurden. Ohne dass dies ersichtlich gewesen sei, habe eine dort installierte Kamera alle ZuschauerInnen erfasst. Die Bilder wurden demnach an eine „Kommandozentrale" in Nashville weitergeleitet, wo sie mit einer Datenbank abgeglichen wurden, in der „Hunderte bekannte Stalker der Sängerin" erfasst waren. Die Sängerin wird seit Jahren von Fans belästigt und bedroht; einige brachen sogar in ihr Haus ein. Swifts Rasterfahndung ist als Notwehrmaßnahme in den USA angeblich legal. Es bestünden aber „offensichtliche Datenschutzbedenken". Was bei einem Fund passiert wäre, wie hoch die Fehlerrate war und ob es überhaupt Treffer gab, wurde nicht bekannt gegeben. Vom Management der Sängerin wurde das Vorgehen nicht kommentiert.

Bei der Veröffentlichung wurde auf den größeren Zusammenhang hingewiesen, dass der Eintrittskartenshop Ticketmaster, eine Tochterfirma des Musikkonzerns Live Nation, Anfang Mai 2018 ein Investment in Blink Identity öffentlich gemacht hatte. Das Unternehmen entwickelt Technik, mit der automatisierte Gesichtserkennung bei Personen funktionieren soll, die sich bewegen. Das soll bei bis zu 60 Personen pro Minute klappen. Damit könnten zuerst einmal VIP-Gäste schneller durch Eintrittskontrollen geschleust werden, hofft Ticketmaster. Man wolle bei der Einführung aber sehr zurückhaltend vorgehen. Die Technik soll 2019 erstmals zum Einsatz kommen und vorerst auf Freiwilligkeit beruhen (Holland, Taylor Swift: Mit heimlicher Gesichtserkennung auf der Suche nach Stalkern, www.heise.de 13.12.2018, Kurzlink: https://heise.de/-4249514; Hurtz, Rasterfahndung im Konzert, SZ 14.12.2018, 9).

China

Kfz-Hersteller liefern Daten von E-Autos

In China funken Elektroautos sensible Informationen nicht nur an die Herstellerfirmen, sondern diese übermitteln die meist personenbezogenen Daten auch an spezielle Auswertungszentren vor Ort, wo sich dann die chinesischen Behörden, u. a. auch die Polizei, bedienen können. An dem Programm beteiligen sich gemäß Presseberichten mehr als 200 Autobauer, zu denen aus Deutschland VW, BMW und Daimler gehören sowie andere globale oder nationale Größen wie Tesla, Ford, General Motors, Nissan, Mitsubishi und das Startup Nio.

Mehr als 61 „Datenpunkte" leiten die Herstellerfirmen gemäß den nationalen Spezifikationen an Institutionen wie das Shanghai Electric Vehicle Public Data Collecting, Monitoring and Research Center. Dazu gehören neben den heiklen Standortinformationen, mit denen sich ausgefeilte Bewegungsprofile erstellen lassen, Details zur Akku- und Motorenfunktion. Gemäß einem Bericht des International Council on Clean Transportation sind die Bestimmungen zum Datentransfer seit Anfang 2017 in Kraft. Im Shanghaier Sammelzentrum werden unter anderem die übermittelten Messwerte genutzt, um nahezu in Echtzeit eine Übersichtskarte vom Fluss von über 222.000 E-Autos, insbesondere PKW, in der Küstenmetropole zu erstellen. Der stellvertretende Leiter der staatlich finanzierten Einrichtung, Ding Xiaohua, erklärte, so könne man die Regierung mit vielen Daten von VerbraucherInnen versorgen, um Peking etwa die Verkehrsplanung zu erleichtern. Auf Ersuchen hin würden die Informationen auch an Sicherheitsbehörden weitergegeben. Bisher sei dies aber erst einmal im Fall eines Autos, das Feuer gefangen habe, der Fall gewesen.

Die Daten fließen dem Bericht zufolge auch an ein nationales Kontrollzentrum für E-Fahrzeuge beim Pekinger Institut für Technologie. Dieses sammle Messwerte von über 1,1 Millionen Pkw, Lkw und Bussen im ganzen Land. Die Zahlen werden voraussichtlich stark zunehmen, da der Anteil der Verkäufe von E-Kfz am Automarkt in China von 2,6% im Jahr 2017 bis 2025 auf 20% ansteigen soll. ExpertInnen gehen davon aus, dass die Fahrzeugdaten auch das staatliche chinesische Überwachungssystem erweitern. Maya Wang von der Menschenrechtsorganisation Human Rights Watch stellte fest: „Die Regierung will jederzeit wissen, was die Leute vorhaben, und darauf möglichst schnell reagieren." Der frühere US-Minister für Homeland Security Michael Chertoff ergänzte, in der Volksrepublik China gebe es keinen Schutz vor staatlichem Ausspähen. Mit den Messwerten lerne man sehr viel über die täglichen Aktivitäten der BürgerInnen, was Teil einer „ubiquitären Überwachung" sei. Die Autoindustrie solle sich selbst fragen, ob es richtig sei, derlei Instrumente einem autoritären Staat verfügbar zu machen.

Ding weist darauf hin, dass sein Zentrum zwar die eindeutige Fahrzeugidentifikationsnummern habe, nicht jedoch die persönlichen Daten der FahrzeughalterInnen. Dafür müsse es sich erst an die Hersteller wenden, was bereits

vorgekommen sei. Die chinesischen Strafverfolger hätten aber einfachere Möglichkeiten, die Informationen über die Halterin oder den Halter zu bekommen. Um die Fahrenden im Blick zu behalten, seien die Sicherheitsbehörden angesichts zahlreicher anderer Mittel wohl gar nicht auf die Bewegungsdaten angewiesen. Zum Plan der Einrichtung gehöre es aber, Big-Data-Analysen und daraus ableitbare Trends zu kommerzialisieren und etwa an Unternehmen zu verkaufen.

Volkswagens China-Chef Jochem Heizmann bestätigte, dass seine Firma Autodaten an ein Regierungssystem liefern muss. Ihren Aufenthaltsort gäben die Leute aber auch schon permanent bekannt, wenn sie ein Smartphone mit sich führten. KäuferInnen müssen laut VW, Daimler und General Motors in China in Vereinbarungen zur Datenweitergabe einwilligen. Tesla wollte den Fall nicht direkt kommentieren und verwies allgemein auf eine eigene, von KundInnen zu bestätigende Richtlinie, dass Fahrzeugdaten gegebenenfalls auf Basis nationaler Gesetze mit Dritten geteilt würden.

Die internationale Datenschutzkonferenz hatte 2017 eine Resolution verabschiedet, wonach Kfz-Nutzende es verhindern können sollen, dass Standort- und Bewegungsdaten aus einem vernetzten Auto weitergegeben werden. Die 120 Aufsichtsbehörden aus 78 Staaten forderten die Hersteller auf, die Privatsphäre der InsassInnen und den Schutz ihrer personenbezogenen Informationen in jeder Phase der Entwicklung und Herstellung neuer Produkte und Dienste sicherzustellen. Unvermeidbare Messwerte sollten möglichst anonymisiert oder pseudonymisiert werden (Krempl, E-Autos: VW, BMW, Daimler & Co. geben Peking Zugriff auf Standortdaten, www.heise.de 02.12.2018).

Simbabwe

Internet „abgeschaltet“

In Simbabwe war es nach einer Verdoppelung des Benzinpreises zu heftigen Protesten gekommen. Aus Furcht vor neuen Protesten der Opposition hat Simbabwes Regierung Mitte Januar 2019 bis auf weiteres eine völlige Abschaltung des Internets angeordnet. Der Schritt sei gerechtfertigt, weil es in sozialen Medien erneut Versuche gebe, Proteste zu organisieren, sagte der stellvertretende Informationsminister Energy Mutodi. Der wichtigste Mobilfunkanbieter, Econet, wehrt sich vor Gericht gegen die Abschaltung. Bis zu einer Klärung müsse man jedoch der Anordnung der Regierung Folge leisten, hieß es. Bei Protesten gegen die drastische Erhöhung der Treibstoffpreise in Simbabwe sind mindestens drei Menschen getötet worden. Mehrere Menschen wurden verletzt. Die Abschaltung des Netzes führte dazu, dass es Probleme gab, die Angestellten im öffentlichen Dienst zu bezahlen, da auch Finanztransaktionen online abgewickelt werden. Auch andere Dienste funktionierten nicht , so dass es auch zu Kollateralschäden bei Flugbuchungen, Hotelbuchungen, dem Datenaustausch zwischen Behörden oder bei der Polizei kam.

Das Abschalten von Netzen wurde in Afrika schon mehrmals vorgenommen. In den Jahren von 2016 bis 2018 sind weltweit 371 Sperrungen dokumentiert. In Afrika ist dies dadurch besonders einfach, dass fast die gesamte Kommunikation per Funk erfolgt. Eine Regierung weist dann die Mobilfunkbetreiber an, das gesamte Netz oder bestimmte Inhalte zu blockieren, etwa den Zugang zu Facebook, WhatsApp oder Twitter. Die Provider filtern dann wie gewünscht die Inhalte aus dem Datenverkehr heraus (Simbabwe schaltet das Internet ab, www.zdf.de 18.01.2019; Wie schaltet man das Internet ab, Herr Holz? Der Spiegel Nr. 5 26.01.2019, 56).

Mosambik

Elektronisches Bezahlsystem fällt aus

Mitte November 2018 verunsicherte in Mosambik über viele Tage hinweg ein Ausfall großer Teile des Karten-Bezahlsystems VerbraucherInnen und Geschäftsleute. Geldautomaten, mobile Kartenleser und Bezahlstationen in Supermärkten, Tankstellen, Krankenhäusern und Hotels akzeptierten nur noch internationale sowie eine einzige nationale Kreditkarte als Zahlungsmittel. KundInnen anderer Banken mussten an Bankschaltern um Bargeld anstehen, um damit ihre Rechnungen zu bezahlen oder einzukaufen. Oder sie mussten auf Handytransfer umsteigen. Das verfügbare Bargeld wurde knapp. Hintergrund ist ein Streit zwischen dem mosambikanischen Bankennetzwerk Simo und dem portugiesischen Softwareprovider Bizfirst. Die KundInnen wurden nicht informiert. Die wirtschaftlichen Folgen waren dramatisch: Supermärkte klagten über Umsatzeinbrüche von bis zu 30%. In Krankenhäusern mussten Operationen verschoben werden, weil die PatientInnen nicht im Vorfeld bezahlen konnten. In den Banken bildeten sich Schlangen vor den Schaltern (Karten-Bezahlsystem fällt aus, SZ 20.11.2018, 18).

Technik-Nachrichten

E-Mail-Adressen mit Passwörtern im Netz zum direkten Abruf

Troy Hunt, Betreiber der Passwort-Sicherheits-Webseite Have I Been Pwned (HIBP), hat eine riesige Sammlung mit E-Mail-Adressen und geknackten Passwörtern im Netz gefunden. Insgesamt finden sich darin knapp 773 Mio. unterschiedliche E-Mail-Adressen und 21 Mio. unterschiedliche Passwörter. In einem Blogpost teilte er mit, dass nach seinen Recherchen ca. 140 Mio. E-Mail-Adressen neu sind. Der Unterschied zwischen den Zahlen erklärt sich dadurch, dass Nutzende dasselbe Passwort für mehr als eine Seite verwenden. In dem Untergrund-Forum, in dem Hunt die Sammlung entdeckte, wurde der Datensatz unter dem Namen „Collection #1“

gehandelt. Die Daten stammen offenbar aus unterschiedlichen Quellen; alle Passwörter liegen im Klartext vor. Bei den betroffenen Webseiten handelt es sich insbesondere um solche mit der Endung .com. Allerdings finden sich auch Daten von etwa 250 deutschen Domains, darunter z. B. mannheim.fruehstueckstreff.de, netzwerk-psychoanalyse.de, primus-versand.de oder strickideen.de

Die Anbieter der Sammlung haben demnach die Daten so strukturiert, dass sie vor allem für „Credential Stuffing" zu gebrauchen sind („Vollstopfen mit Anmeldedaten"). Bei dieser Art Angriff auf eine Webseite versucht der Angreifer nicht das Passwort eines einzelnen Accounts zu knacken, sondern füttert den Login-Mechanismus automatisch mit E-Mail- und Passwort-Kombinationen aus einer großen Liste. Die Listen, die in dem Datenleck enthalten sind, stellen fast 2,7 Milliarden solcher Kombinationen zur Verfügung. Angreifer können sie nutzen, um massenweise Konten bei Webdiensten zu übernehmen. Das hat oft Erfolg, da viele Nutzende dieselben Kombinationen von Mailadressen und Passwörtern bei vielen Diensten wiederverwenden.

Hunt hält es für plausibel, dass die Angaben der Verkäufer in dem Untergrund-Forum stimmen und die Daten aus vielen verschiedenen Hacks und Passwort-Leaks aus der Vergangenheit zusammengetragen wurden. Aus der Verzeichnisstruktur des Datensatzes ließen sich Schlüsse über Webseiten ziehen, aus denen die Daten stammen könnten. Bei allen diesen Diensten Nachforschungen anzustellen, ob und wann sie gehackt wurden, scheine aber eine fast unlösbare Aufgabe zu sein, v. a. weil man dafür auf die Kooperation jedes einzelnen Dienstes angewiesen wäre.

Wer wissen will, ob eine seiner Mailadressen mit dazugehörigem Passwort in der Datensammlung vorkommt, der kann Hunts Dienst HIBO nutzen, wo die Daten eingepflegt sind. Allerdings sagt eine Anfrage dem Anwendenden nur, ob eine Mailadresse in dem Leak vorkommt. Hunt speichert aus rechtlichen und rein logistischen Gründen keine Passwörter in seinem Dienst, sondern nur Hashes von Mailadressen, die kompromittiert wurden. Ist die Adresse allerdings im Collection-#1-Datensatz, sollte man gemäß der Empfehlung Hunts das dazugehörige Passwort ändern.

Einzelne Passwörter lassen sich mit der Funktion Pwned Passwords der Seite überprüfen. Die Webseite sagt dem Anfragenden dann, ob das Passwort schon mal in einem bekannten Datenleck aufgetaucht ist. Auch hier speichert Hunt nur Hashes und keine Passwörter im Klartext und überträgt nur Teile der Hashes, damit er selbst und ein mithörender Angreifer nicht auf das eingegebene Passwort schließen können. Hunt gibt sich offenbar alle Mühe, die Daten, die an seine Seite übermittelt werden, nach dem aktuellen Stand der Technik zu schützen. Trotzdem gilt grundsätzlich die Regel: Gib niemals ein Passwort irgendwo auf einer Webseite ein, außer es handelt sich um das Passwort-Feld der Seite, zu der es gehört.

Wenig später nach Veröffentlichung dieses Leak haben IT-ExpertInnen des Potsdamer Hasso-Plattner-Instituts (HPI) weitere riesige Sammlungen von ungesicherten Zugangsdaten im Internet gefunden. Zu den rund 770 Millionen E-Mail-Adressen und Passwörtern kamen noch einmal etwa 1,5 Milliarden Datensätze hinzu. Diese neuen Daten sind offenbar weitere Teile des vorangegangenen Lecks. Mitarbeiter des HPI haben die neu entdeckten Zugangsdaten in eine Datenbank eingepflegt, Internetnutzende können auf der Seite sec.hpi.de/ilc/ ihre E-Mail-Adresse eingeben. Das Institut gleicht diese dann mit den Daten in dem Leak ab und schickt eine Auswertung per Mail. Wer betroffen ist, sollte sein Passwort auf betroffenen Seiten ändern.

Hunt empfiehlt Nutzenden, einen Passwort-Manager zu benutzen und dafür zu sorgen, dass jede Webseite ihr eigenes Passwort hat. Das sollte beim Leak des Passworts bei einem Anwendenden verhindern, dass Hacker Passwortlisten verwenden können, um Konten bei anderen Diensten zu knacken. Er empfiehlt den Passwort-Manager 1Password, der seinen Dienst HIBP bereits integriert hat. Als andere gute Alternative wird das quelloffene Community-Projekt KeePass genannt. Die beste Verteidigung es aber, viele unterschiedliche starke Passwörter zu verwenden (Scherschel, Passwort-Sammlung mit 773 Millionen Online-Konten im Netz aufgetaucht, www.heise.de 17.01.2019, Kurzlink: https://heise.de/-42793; Brühl/Muth, Millionen ,Passwörter stehen im Netz, SZ 18.01.2019, 24; Neue Passwort-Leaks, SZ 26./27.01.2019, 26).

Tracking-Studie offenbart umfassende Netzüberwachung

Gemäß einer aktuellen großangelegten Studie geben neun von zehn Android-Apps Informationen ihrer Nutzenden an Drittfirmen weiter. Viele der Apps senden Daten nicht bloß an ein Unternehmen, sondern gleich an mehrere, die fast immer ihren Sitz in den USA haben. Das Sammeln der Nutzungsdaten über die Smartphone-Apps dient der zielgenauen Werbeansprache durch die Drittfirmen. Die beiden größten Verwerter heißen Google und Facebook. Für ihre Studie haben die Forschenden der Universität Oxford und des Reuters Institute for the Study of Journalism knapp eine Million Apps heruntergeladen und deren Code untersucht. Nur etwa 10% der Apps erfassten keine Daten ihrer Nutzenden. Viele der Apps senden Daten nicht bloß an ein Unternehmen, sondern an viele. Die weitaus meisten davon sitzen in den USA. Gut 90% aller Apps mit mindestens einer Verbindung zu einem Datensammler senden Daten an ein US-Unternehmen. Gut 5% kommunizieren mit chinesischen Firmen. Überraschungs-Dritter ist Norwegen mit 3,2%. Deutschland (2,6%) erscheint an fünfter Stelle, nach Russland (ebenfalls 2,6%). Gut 88% aller Apps senden Daten an Google, den Hersteller des Betriebssystems Android. Die Stellung von Google ist hier sogar dominanter als bei normalen Computern.

Das Sammeln von Nutzungsdaten über Computer wie über Smartphones ist keineswegs neu. Während Nutzende bei Computern noch gewisse Möglichkeiten haben, sich zu schützen, haben sie bei Smartphones kaum eine Chance. Das Problem wird dadurch verstärkt, dass PCs oft von mehreren Menschen genutzt werden, Smartphones dagegen sehr persönliche Geräte sind. Durch ihre zahlreichen Sensoren und die vielfältigen Funktionen, die sie erfüllen, sind die Daten, die über sie gesammelt werden, von höherem Wert als die von normalen Computern. Je

mehr Daten von möglichst vielen Nutzenden ein Unternehmen sammeln kann, desto genauer kann es mit Big-Data-Algorithmen Einstellungen, Vorlieben und mögliches künftiges Verhalten der Nutzenden berechnen und prognostizieren. Für Werbetreibende ist das von höchstem Interesse, weil sie damit ihre potenziellen KundInnen zielgerichtet ansprechen und manipulieren können.

Das Forscherteam um Reuben Binns stellte fest, dass die meisten Apps mit mehreren Datensammel-Firmen verknüpft sind, die wiederum oft zu unterschiedlichen Mutterfirmen gehören. Die Forschenden empfehlen daher Aufsichtsbehörden, sich weniger auf Apps zu stürzen als auf die Firmen, die hinter den Datensammlern stehen. Viele der angewandten Praktiken sind gesetzeswidrig, so etwa die Erstellung von Profilen von Kindern. Die europäische Datenschutzgrundverordnung verbietet das, wenn durch Verhaltensanalyse signifikante Effekte auf die Nutzenden entstehen können. Aus der Studie ergibt sich, dass die Regulierung des Trackens äußerst komplex ist, da viele Akteure beteiligt sind, Nutzende, Gerätehersteller, Betriebssystemhersteller, die Entwickler der Apps und die Tracking-Firmen, die jeweils verschiedene Interessen verfolgen und verschiedene Möglichkeiten haben: „Eine wirksame Regulierung erfordert Zusammenarbeit zwischen den Regulatoren und dieser Myriade anderer Akteure“ (Martin-Jung, Jäger und Sammler, SZ 05.11.2018, 18).

Google-Tochter Verily stoppt Glukose-messende Kontaktlinse

Den Glukosespiegel in der Tränenflüssigkeit zu messen, ist nicht so einfach, wie die Google-X-Entwickler von Verily, Alphabets Abteilung für Life Sciences, sich das vorgestellt haben. Sie haben deshalb die Arbeit an einer Kontaktlinse für Diabetes-PatientInnen eingestellt. Das System lieferte nicht die gewünschten Ergebnisse.

Vor vier Jahren hatte das Forschungslabor Google X das Konzept einer mit Sensoren ausgestatteten Kontaktlinse vorgestellt. Diese sollte den Blutzuckerspiegel in der Tränenflüssigkeit messen und zwar in Sekundenabständen, so dass die TrägerInnen ihren Zuckerspiegel beinahe in Echtzeit hätten überwachen können. Der Pharmakonzern Novartis wollte die Kontaktlinse in Serie herstellen (vgl. DANA 2014, 81). Die EntwicklerInnen von Verily resümierten nun: „In unserer klinischen Arbeit mit der Glukose-messenden Linse hat sich gezeigt, dass die Messungen des Glukosewerts in der Tränenflüssigkeit und im Blut nicht genug Übereinstimmung aufwiesen, um die Anforderungen an ein medizinisches Gerät zu erfüllen.“ Daher habe man sich dazu entschlossen, dieses Projekt erst einmal zu stoppen. Verily wolle jedoch weiter an smarten Kontaktlinsen arbeiten, ebenso an Projekten zur Behandlung von Diabetes. Ziel sei es, eine unauffällige und günstige Methode zur Messung des Zuckerspiegels zu entwickeln. Verily war im Zuge des Konzernumbaus von Google im Jahr 2015 in ein eigenes Unternehmen ausgegliedert worden (Pluta, Verily: Alphabet stoppt Arbeit an Glukose-messender Kontaktlinse, www.golem.de 17.11.2018).

Suchmaschine Startpage.com mit anonymer Surffunktion

Die datenschutzfreundliche Suchmaschine „startpage.com“ hat eine „Anonyme Ansicht“-Funktion entwickelt. Sie schützt die UserInnen vor Tracking, indem sie nicht nur beim Suchen, sondern auch beim Aufrufen einer Seite einen anonymisierenden Puffer zwischen Websites und Usern schafft.

Während z. B. der Inkognito-Modus nicht vor Tracking oder dem Speichern und Verkaufen der persönlichen Daten schützt, soll dies gemäß Unternehmensangaben bei der „Anonymen Ansicht“ gewährleistet sein. Dabei besucht Startpage anstelle der UserIn selbst die von ihr ausgewählte Website und zeigt sie der UserIn anonym an. Die besuchte Website sieht nur Informationen von Startpage, während die UserIn selbst für den Webseitenbetreiber unsichtbar bleibt. Die „Anonyme Ansicht“ ist kostenlos und befindet sich rechts neben dem jeweiligen Suchergebnis.

Startpage-CEO Robert Beens erklärte: „Anders als beim Inkognito-Modus schützt die Anonyme Ansicht wirklich. Sie kombiniert Suchen in Privatsphäre mit Surfen in Privatsphäre. Wir werden weiterhin die besten Suchergebnisse ohne Tracking und Profiling anbieten.“ Sein Unternehmen hat seinen Sitz in Europa, zeichnet sich durch eine anonyme Suche im Internet aus und verspricht, keine persönlichen Daten oder Userprofile zu speichern (PE Startpage.com 29.11.2018).

Rechtsprechung

BVerfG

Strafverfolgungszwecke zwingen E-Mail-Anbieter zur IP-Speicherung

Das Bundesverfassungsgericht (BVerfG) in Karlsruhe hat mit Beschluss vom 20.12.2018 bestätigt, dass auch E-Mail-Anbieter, die mit hohem Datenschutz werben, mit Strafverfolgern kooperieren und auf Anfrage IP-Adressen nennen müssen (Az. 2 BvR 2377/16). Demgemäß müssen sie Strafverfolgern IP-Adressen von Nutzenden mitloggen und mitteilen, auch wenn sie diese normalerweise nicht protokollieren. Die Tatsache, dass diese Adressen im Sinne der Grundrechte durchaus schutzwürdig sind, stehe dem nicht im Weg. Die dritte Kammer des BVerfG wies damit eine Klage des Mailproviders Posteo als unzulässig und teils unbegründet ab.

Der E-Mail-Anbieter wirbt für seine Dienste mit besonderer Datensparsamkeit. Posteo zeigt via Network Adress Translation (NAT) die IP-Adressen nicht

nach außen an und speichert diese jeweils nur sitzungsbezogen sowie temporär in einer internen Datenbank. Als die Staatsanwaltschaft Stuttgart 2016 anklopfte und wegen eines Verdachts auf Verstöße gegen das Betäubungsmittel- und Kriegswaffenkontrollgesetz Telekommunikationsdaten eines Kunden haben wollten, erklärte der Provider, die IP-Adressen nicht liefern zu können.

In den sich anschließenden Verfahren vor dem Amtsgericht und dem Landgericht Stuttgart hielten die Posteo-Anwälte den Gerichten unter anderem entgegen, dass auch die sogenannte Infrastrukturpflicht (§ 110 TKG), mit der Provider zum Vorhalten von Überwachungstechnik verpflichtet wird, keine klare Rechtsgrundlage für die Erhebung der IP-Adressen beinhalte. Das BVerfG folgte den Vorinstanzen und unterstrich, dass IP-Adressen wie andere Verkehrsdaten unter den Sammelbegriff „andere Adressierungsangabe“ (§ 7 Abs.1 Satz 1 Nr. 4 TKÜV) fallen. Bei Straftaten erheblicher Bedeutung könnten die Strafverfolger die IP-Adressen daher verlangen. Das bedeutet nach Ansicht der Verfassungsrichter „nicht zwangsläufig, dass der Beschwerdeführer als Betreiber einer Telekommunikationsanlage verpflichtet ist, Vorkehrungen zu treffen, um den Ermittlungsbehörden auch und gerade diese IP-Adressen zur Verfügung zu stellen.“ Die fallbezogene Herausgabe ab Mitteilung, so der Schluss, genüge.

Der Provider hatte das gegen ihn verhängte, bescheidene Ordnungsgeld von 500 Euro längst bezahlt, machte aber geltend, dass die von ihm verlangte Maßnahme für ihn teuer werden kann. Eine etwa über 12 Monate laufende Überwachungsmaßnahme schlage bei Beibehaltung seines datensparsamen Systems mit rund 80.000 Euro zu Buche. Die Richter des BVerfG erkennen an, dass der Beschwerdeführer Sanktionen künftig eben nur durch „erhebliche, zeit- und kostenintensive Umbauarbeiten vermeiden kann.“ Dies sei aber „lediglich eine Folge der vom Beschwerdeführer bewusst gewählten Systemstruktur“. Die Wahl eines datenschutzoptimierten Geschäftsmodells könne den Beschwerdeführer nicht von der Einhaltung der Koorperationspflichten mit Strafverfolgern suspendieren. Auf eine mögliche Existenzbedrohung hatte das Unternehmen nicht verwiesen. Für kleine oder neu auf dem Markt kommende Mailanbieter oder andere Provider, die auf besonders hohen Datenschutz setzen, könnte das allerdings anders aussehen.

Posteo zeigte sich „sehr überrascht“ von der Entscheidung, die die bisherige rechtliche Auskunftssystematik auf den Kopf stelle: „Bisher war unbestritten, dass sich die Auskunftspflicht nur auf Daten bezieht, die bei TK-Anbietern nach § 96 TKG tatsächlich auch vorliegen. Nun sollen Daten auch alleinig zu Ermittlungszwecken erhoben werden: Daten, die beim TK-Anbieter im Geschäftsbetrieb nachweislich so gar nicht anfallen – und die er im Geschäftsbetrieb auch nicht benötigt“. Posteo will nach dem Beschluss nun nicht damit beginnen, die IP-Adressen der KundInnen zu loggen: „Ein konservativer System-Umbau ist für uns keine Option“ (Ermert, Bundesverfassungsgericht: Mail-Provider muss IP-Adressen herausgeben, www.heise.de 29.01.2019, Kurzlink: https://heise.de/-4291456).

BSG

Foto-Löschung nach eGK-Herstellung rechtlich geboten

Gemäß einem Urteil des Bundessozialgerichts (BSG) in Kassel vom 18.12.2018 müssen Krankenkassen nach Herstellung einer „elektronischen Gesundheitskarte“ (eGK) das hierfür verwendete Foto wieder löschen, da die bislang übliche dauerhafte Speicherung ohne Zustimmung des Versicherten gegen Datenschutzrecht verstößt (Az.: B 1 KR 31/17).

Die eGK wird seit 2013 von den Krankenkassen ausgegeben und muss seit Anfang 2014 genutzt werden. Seit 2015 dürfen die medizinischen Leistungserbringer für die Kostenabrechnung keine anderen Nachweise mehr anerkennen. Die Karten haben ein Foto des Versicherten und einen Speicherchip. Auf diesem sind bislang nur dieselben „Stammdaten“ gespeichert, die auch schon früher auf der Krankenversichertenkarte aufgedruckt waren, darunter Name, Geburtsdatum, Anschrift und Geschlecht. Künftig sollen auch weitere Daten gespeichert werden, etwa die Blutgruppe, Allergien und andere wichtige Krankheiten. Die Fotos sollen insbesondere Missbrauch verhindern. Die Krankenkassen speichern diese bislang routinemäßig bis zum Ende des Versicherungsverhältnisses und verwenden sie auch für spätere Ausfertigungen oder für Ersatzkarten.

Ein Mitglied der Techniker Krankenkasse sah dadurch sein Recht auf informationelle Selbstbestimmung verletzt. Mit seiner Klage verlangte er zuletzt noch die Löschung des Fotos nach Herstellung der Karte. Die Techniker Krankenkasse meinte, die Fotos würden sicher gespeichert, und der Datenschutz sei gewährleistet. Durch eine Löschung würden unnötige Kosten entstehen. Schon jetzt würden jeden Tag etwa 10.000 Fotos an die Kasse geschickt. Darunter seien auch Ulkbilder, etwa mit einem Teddybären oder einem Pinguin. Die Fotos müssten daher stets überprüft und technisch verarbeitet werden. Im Gegensatz zu den Vorinstanzen stellte das BSG fest, dass jedenfalls ohne Zustimmung des Versicherten die Datenschutzregelungen eine Verarbeitung und Speicherung persönlicher Daten und damit auch des Fotos nur für den jeweils konkreten Zweck – hier also die Herstellung der Gesundheitskarte erlaubten. Danach müssten die Krankenkassen das Foto löschen. Dass die Versicherten den Krankenkassen aber grundsätzlich ein Foto zur Verfügung stellen müssen, hatte das BSG bereits am 18.11.2014 entschieden (B 1 KR 35/13 R). Das Foto sei „geeignet und erforderlich, um missbräuchlichen Nutzungen zu begegnen“ (Bertram, Krankenkassen dürfen Versichertenfoto nicht dauerhaft speichern, www.heilpraxisnet.de, 19.12.2018).

OVG Bremen

Moscheebesuch kein Grund für Einbürgerungsverweigerung

Mit Beschluss vom 09.11.2018 entschied das Oberverwaltungsgericht (OVG) Bremen, dass der wiederhol-

te Besuch einer vom Amt für Verfassungsschutz (VerfSch) beobachteten Moschee kein Grund ist, dem Besucher die Einbürgerung in Deutschland zu verweigern (1 LA 78/17). Die Hansestadt hatte den Einbürgerungsantrag des Ausländers zuvor abgelehnt, weil dieser zwischen 2009 und 2013 nach Feststellungen des VerfSch 17-mal das Freitagsgebet des Islamischen Kulturzentrums (IKZ) besucht und dort auch Geld gespendet hatte. Das IKZ galt seit Langem als Treffpunkt fundamentalistischer Salafisten. 2017 hatte bereits das Verwaltungsgericht Bremen in erster Instanz entschieden, dass die Stadt die Einbürgerung nicht aus diesen Gründen ablehnen darf. In der Moschee gebe es nicht nur fundamentalistische, sondern auch andere Strömungen. Spenden bei Freitagsgebeten seien üblich; es gebe keine Anhaltspunkte dafür, dass der Besucher damit die „vermutlich verfassungsfeindliche Tätigkeit des IKZ" unterstützen wollte. Vielmehr habe sich der Mann vor Gericht klar zur freiheitlich-demokratischen Grundordnung bekannt (Moscheebesucher darf Deutscher werden, Der Spiegel Nr. 46 10.11.2018, 13).

VG München

Airbnb auskunftspflichtig über Kurzzeitvermieter

Gemäß einem Urteil des Verwaltungsgerichts (VG) München vom 12.12.2018 muss Airbnb der Stadt München Daten zu Ferienwohnungen, die maximal acht Wochen im Jahr vermietet werden dürfen, offenlegen (M 9 K 18.4533).

Große Städte in Deutschland versuchen verstärkt, gegen die zunehmende Zweckentfremdung von Wohnungen als Ferienwohnungen vorzugehen. Das VG München bestätigte die Rechtmäßigkeit der Forderung der bayerischen Landeshauptstadt gegenüber Internetanbietern wie Airbnb, umfassend über Wohnungen, die mehr als acht Wochen lang auf den Plattformen zur Vermietung an Feriengäste angeboten werden, Auskunft zu geben. Der Umstand, dass Airbnb seinen Firmensitz in Irland habe, ändert nichts daran, dass sich die Internetplattform an die in Deutschland geltenden Vorschriften halten muss. Vor Gericht hatte das US-Unternehmen sich darauf berufen, dass wegen seines europäischen Sitzes in Dublin laut Telemediengesetz (TMG) bei Geschäften in der EU nur irisches Recht gelte und nicht bayerisches. Das Gericht bestätigte die Geltung der nationalen Vorschriften, da das Unternehmen hier tätig ist. Irland sei nicht für die Umsetzung des bayerischen Zweckentfremdungsgesetzes zuständig. Airbnb sei als Wohnungsvermittlerin dazu verpflichtet, die Stadt dabei zu unterstützen, illegal vermietete Wohnungen aufzuspüren und Auskunft über deren Anbieter zu erteilen. Die Stadt verlangte vom Betreiber der Plattform die Anschriften der angebotenen Wohnungen nebst Namen und Adressen der Gastgeber für den Zeitraum von Januar 2017 bis Juli 2018. Für den Fall, dass Airbnb sich weigert, hatte die Stadt im August 2018 mit einem Zwangsgeld von 300.000 € gedroht. Auch das ist gemäß dem VG München rechtens.

Nach Angaben des Sozialreferats der Stadt München werden immer mehr Wohnungen für Feriengäste über Internetportale angeboten. Um Zweckentfremdungen zu bekämpfen, setzte die Behörde ein Sonderermittlungsteam ein, das im Jahr 2017 bereits 21.000 Wohnungen untersuchte. Mitte Januar 2018 ging eine Meldeplattform online, wo verdächtige Wohnungen etwa in der Nachbarschaft mitgeteilt werden können. Im ersten Jahr waren so mehr als 1.000 Hinweise eingegangen. 298 Wohnungen führte die Stadt gemäß eigenen Angaben dem Wohnungsmarkt wieder zu. Es wurden 92 Gerichtsverfahren zu Gunsten der Städte entschieden und Bußgeldbescheide in Höhe von 851.110 Euro erlassen. Die Daten von Airbnb sollen von dem Ermittlungsteam „Raum für München" mit den registrierten Ferienwohnungen abgeglichen werden, um die mutmaßlich illegalen herauszufiltern.

Münchens Oberbürgermeister Dieter Reiter begrüßte, „dass sich Airbnb nicht aus der Verantwortung ziehen kann". Jede bezahlbare Wohnung werde für die Münchnerinnen und Münchner gebraucht. Das Urteil vom VG könnte auch anderen Städten eine Orientierung bieten, die ebenfalls gegen Zweckentfremdung kämpfen. Airbnb prüft nun maximal einen Monat, ob es Berufung einlegt. Eine Sprecherin erklärte, der Schutz der Nutzerdaten habe höchste Priorität. Man wolle aber weiter mit München zusammenarbeiten, um „gemeinsam einen effektiven Wohnraumschutz zu unterstützen und gleichzeitig dazu beizutragen, dass Münchner ihr Zuhause mit Reisenden teilen können".

Die Rechtslage bei der Zweckentfremdung ist in den Städten unterschiedlich, so dass das Urteil nicht eins zu eins auf sie übertragen werden kann. Auch in Berlin und Hamburg versuchen die Behörden, mit Ermittlungen und Bußgeldandrohungen gegen Zweckentfremdungen vorzugehen (Airbnb muss Identität von Vermietern herausgeben, www.zeit.de 13.12.2018; Kohrs, Airbnb muss Gastgeber preisgeben, SZ 14.12.2018, 28).

OLG Hamburg

Marktverhaltensregelnde Datenschutznormen sind abmahnfähig

Das Oberlandesgericht (OLG) Hamburg hat mit Urteil vom 25.10.2018 als erstes OLG bundesweit entschieden, inwieweit Verstöße gegen die Datenschutz-Grundverordnung (DSGVO) wettbewerbsrechtlich abgemahnt werden können. Es kommt dabei grundsätzlich zu einem positiven Ergebnis (3 U 66/17). Abmahnungen sind bei Datenschutzverstößen demnach nur möglich, wenn sich Unternehmen durch den DSGVO-Verstoß einen Vorteil im Wettbewerb verschafft haben. Deutsche Gerichte sind sich bisher in dieser Frage uneins (vgl. DANA 4/2018, 223 f. mit Hinweisen auf die Entscheidungen des LG Würzburg und des LG Bochum). Bei der Entscheidung aus Hamburg ging es um zwei Pharmaunternehmen, die sich wegen Verstößen gegen das Datenschutzrecht gegenseitig verklagt hatten. Nach Ansicht des OLG muss im Einzelfall jeweils die Regelung in der DSGVO daraufhin überprüft werden, ob sie eine Marktverhaltensregel zum Gegenstand hat. Ist das der Fall, können Mitwerber Verstöße nach Einschätzung der Hamburger Richter wettbewerbsrechtlich abmahnen. Es kommt also darauf an, ob sich Unternehmer durch den Rechtsver-

stoß einen Wettbewerbsvorteil gegenüber ihrer Konkurrenz verschafft haben. Ist dies der Fall, so können Mitbewerber gemäß § 3a UWG (Gesetz gegen den unlauteren Wettbewerb) abmahnen. Es kann also nicht pauschal vorgegangen werden. Vielmehr hängt es gemäß dem OLG davon ab, ob die jeweilige DSGVO-Regelung als Marktverhaltensregelung angesehen wird, was letztlich der Bundesgerichtshof (BGH) höchstrichterlich feststellt.

Das erstinstanzliche Urteil hatte das Landgericht Hamburg im Fall der Pharmaunternehmen bereits im März 2017 gefällt – also mehr als ein Jahr, bevor die DSGVO europaweit verbindlich wurde. Da Unterlassungsansprüche in die Zukunft gerichtet sind, werden diese anhand der Normen geprüft, die zum Zeitpunkt der mündlichen Verhandlung gelten. Die Verhandlung vor dem OLG Hamburg fand am 25.10.2018 statt, also als die DSGVO genau fünf Monate anwendbar war (Leupold, Oberlandesgericht sagt „vielleicht" zu DSGVO-Abmahnungen, www.handwerk.com 30.11.2018).

LG Bonn

WHOIS-Domain-Datenbank ist nicht DSGVO-konform

Das Landgericht (LG) Bonn wies mit Beschluss vom 29.05.2018 einen Antrag auf einstweilige Anordnung gegen den in Deutschland beheimateten Registrar EPAG zurück, über den EPAG verpflichtet werden sollte, Kontaktdaten von Tech-C und Admin-C zu erheben und der Internetverwaltung ICANN zur Verfügung zu stellen (Az. 10 O 171/18). In der europäischen Datenschutzgrundverordnung (DSGVO) ist der Grundsatz der Datensparsamkeit verankert. Diesem kommt die Internetverwaltung ICANN mit ihrer Domain-Registrierungsdatenbank WHOIS nicht nach. Wer eine Internetadresse registrieren will, kommt an der US-amerikanischen Internetverwaltung Internet Corporation for Assigned Names and Numbers (ICANN) nicht vorbei. Diese hatte Mai 2018 ein Gerichtsverfahren gegen die EPAG Domainservices GmbH, ein zur Tucows-Gruppe gehörender Registrar mit Sitz in Bonn, eingeleitet. Grund dazu gab die unterschiedliche Interpretation von Tucows und ICANN bezüglich der Auslegung der DSGVO.

Der Registrar-Akkreditierungsvertrag der ICANN in der Fassung von 2013 verpflichtete, so der Beschluss, zur Erhebung nicht erforderlicher Daten. So wurden bisher beispielsweise personenbezogene Daten von Personen verlangt, zu denen kein direkter Bezug besteht, wie die Admin- und Tech-Kontakte – also der technischen sowie administrativen Domainverwaltung. Anhand der bei ICANN gespeicherten Daten konnte bisher zudem ein Domaininhaber ganz einfach über eine WHOIS-Abfrage ermittelt werden, indem der Rechteinhaber auf der Website des Registrars die entsprechende Web-Adresse eingab. Sofort erhielt man Informationen über die Identität des Domaininhabers und den Ansprechpartner für technische und administrative Belange dieser Domain. Die WHOIS-Domain-Datenbank verstößt demnach also in ihrer ursprünglichen Form gegen die DSGVO. Entsprechend hat die Tuscows-Gruppe ihr Formular den europäischen Datenschutzrichtlinien angepasst.

ICANN hatte argumentiert, die Fragmentierung der WHOIS-Datenbank bedeute eine potenzielle Gefahr. So könnten Cyberkriminelle davon profitieren. ICANN forderte deshalb eine Ausnahme von der Datenschutz-Grundverordnung, so ihr Präsident Göran Marby: „Wir prüfen alle verfügbaren Möglichkeiten, einschließlich rechtlicher Schritte in Europa, um auch weiterhin diese wichtige globale Informationsressource koordinieren zu können." Gemäß dem Beschluss des LG konnte ICANN nicht glaubhaft darlegen, dass das Speichern jener Daten, die über die Information des Domaininhabers hinausgehen, erforderlich seien. Man könne gemäß dem in der DSGVO verankerten Grundsatz der Datensparsamkeit nicht erkennen, wozu zusätzliche Daten erhoben werden. Die ICANN hatte eingeräumt, dass Domains registriert werden können, wenn diese drei Datensätze identisch sind. Mit dem Beschluss scheint der Streit über die Umsetzung der DSGVO noch nicht beendet zu sein. Die ICANN erklärte, sich deshalb sowohl mit der EU-Kommission als auch mit dem europäischen Datenschutzbeauftragten in Verbindung zu setzen (Gandorfer, WHOIS-Domain-Datenbank nicht DSGVO-konform, www.it-business.de, 02.10.2018).

LG Berlin

Mieter hat Beseitigungsanspruch wegen Kameraattrappe

Das Anbringen einer täuschend echten Kameraattrappe im Hauseingang durch den Vermieter ist gemäß einem Urteil des Landgerichts (LG) Berlin vom 14.08.2018 dann nicht zulässig, wenn weniger einschneidende Möglichkeiten des Eigentumsschutzes bestehen (67 S 73/18). Ein milderes Mittel könne etwa eine zuverlässig und schnell ins Schloss fallende Eingangstür darstellen. In dem zugrunde liegenden Fall wehrte sich ein Wohnungsmieter in Berlin gegen das Anbringen einer Video-Überwachungskameraattrappe im Hauseingang durch den Vermieter. Die Kameraattrappe wirkte täuschend echt. Durch diese sollte ein Zutritt von Obdachlosen ins Haus verhindert werden. Diese hatten in der Vergangenheit im Haus genächtigt. Der Mieter fühlte sich durch die Kameraattrappe überwacht und klagte auf Entfernung des Geräts.

Das Amtsgericht (AG) Berlin-Mitte hatte als Vorinstanz die Klage abgewiesen. Seiner Auffassung nach sei wegen der bloßen Attrappeneigenschaft der Videokamera kein Eingriff in das allgemeine Persönlichkeitsrecht des Mieters. Hiergegen hatte der Mieter Berufung eingelegt. Das LG entschied zu Gunsten des Mieters und hob die Entscheidung des AG auf. Dem Mieter stehe ein Anspruch auf Entfernung der Video-Überwachungskameraattrappe zu. Die Installation der Kamera stelle einen nicht gerechtfertigten Eingriff in das allgemeine Persönlichkeitsrecht des Mieters dar. Da die Kameraattrappe täuschend echt wirkte und somit von außen nicht ersichtlich gewesen sei, ob eine bloße Attrappe oder eine Videokamera-Anlage mit Aufzeichnung betrieben werde, habe ein unzulässiger Überwachungsdruck vorgelegen.

Zwar dürfe ein Vermieter zum Eigentumsschutz Maßnahmen ergreifen. Da-

bei müsse er aber den Verhältnismäßigkeitsgrundsatz beachten. Im vorliegenden Fall habe eine weniger einschneidende Möglichkeit des Eigentumsschutzes bestanden. Als milderes, aber gleich effektives Mittel sei eine technische Veränderung der Haustür in Betracht gekommen, durch die sichergestellt werden könne, dass die Tür schnell ins Schloss falle. Dadurch könne ein ungewollter oder unberechtigter Zutritt unbefugter Dritter verlässlich verhindert werden (Täuschend echte Kameraattrappe im Hauseingang bei weniger einschneidenden Möglichkeiten des Eigentumsschutzes unzulässig, www.kostenlose-urteile.de 16.11.2018; Überwachungsdruck, SZ 16.11.2018, 32).

Buchbesprechungen



Simitis, Spiros/Hornung, Gerrit/
Spieker gen. Döhmann, Sarah (Hrsg.)
Datenschutzrecht – DSGVO mit BDSG
Nomos Baden-Baden 2019, ISBN 978-3-8487-3590-7, 1474 S., 198 €

(tw) Der neue „Simitis" war schon lange angekündigt; er kommt spät – die Konkurrenz lieferte früher und teilweise schon in der zweiten Auflage – aber nicht zu spät. Spiros Simitis, der Doyen des deutschen Datenschutzes und der einzig Übriggebliebene aus der allerersten Generation des deutschen Datenschutzes, steuert außer seinem guten Namen in dem DSGVO-Kommentar Passagen der Einleitung bei, die teilweise aus dem allein von ihm herausgegebenen Vorwerk, der 8. Auflage des großen BDSG-Kommentars, übernommen wurden. Aus diesem Werk gibt es wenige weitere Bekannte, etwa Alexander Dix, Eugen Ehmann, Thomas Petri, Philip Scholz oder Achim Seifert. Hinzu gekommen sind außer dem neuen Herausgebern weitere einschlägige ExpertInnen: Jan Philipp Albrecht, Franziska Böhm, Johannes Caspar, Stefan Drewes, Marit Hansen, Moritz Karg, Jan Hendrik Klement, Sven Polenz, Alexander Roßnagel, Peter Schantz, Stephanie Schiedermair, Christoph Schnabel. Die meisten der Genannten sind nicht nur hier präsent, sondern in anderen, teilweise eigenen, teilweise fremd herausgegebenen Werken.

Während in allen anderen EU-Staaten eher gähnende Leere hinsichtlich der Literatur zur Datenschutz-Grundverordnung (DSGVO) festzustellen ist, läuft der deutsche Markt dazu über. Hintergrund dieser besonderen literarischen Bearbeitung ist sicher, dass die Einführung der DSGVO hierzulande mit dem größten Trara erfolgte – was nicht zum Schaden eines wirksamen Datenschutzes sein muss.

Natürlich stellt sich nun die Frage, weshalb denn nun die Anschaffung dieses nicht gerade preisgünstigen Kommentars nötig ist: Was dagegen spricht ist, dass – entgegen dem Versprechen des Buchcovers – keine konsistente Kommentierung des neuen BDSG erfolgt; hierzu gibt es lediglich eine Referenzliste, die auf die DSGVO-Kommentierungen verweist. Etwas kompensiert wird dieses Defizit durch von Scholz und Ehmann kommentierte ausführliche Anhänge zu Art. 6 zu den Themen Videoüberwachung, Verbraucherkredite/Scoring/Bonitätsauskünfte, Werbung sowie Markt- und Meinungsforschung, die teilweise eine Vollkommentierung dazu gehöriger BDSG-Paragrafen bringen. Für eine PraktikerIn, die schnell einfache Antworten haben möchte, sind sowohl die Struktur wie auch der Umfang eine gewisse Hürde.

Der Umfang ist dann aber insbesondere auf der Habenseite zu verbuchen: Der Kommentar liefert, ebenso wie ehedem der frühere „BDSG-Simitis" die ausführlichste und am tiefsten gehende Darstellung und greift dabei in großem Umfang auf schon vorliegende Kommentare zurück. Hat man diesen Kommentar, braucht man keine anderen Werke, insbesondere wenn eine datenschutzfreundliche Auslegung gesucht wird, wofür die AutorInnen fast durchgängig stehen. Doch auch insofern teilt das neue Werk einen Nachteil des alten „Simitis": Datenschutz ist heutzutage insbesondere auch Internetdatenschutz, der bisher – wenig befriedigend – in Deutschland im TMG und im TKG geregelt ist. Zwar wird hierauf wie auch auf die geplante Folgeregelung der ePrivacy-Verordnung eingegangen, doch werden dabei wenig praktische Hilfen gegeben.

Das große Plus des „Simitis/Hornung/Spiecker" ist die Qualität der Kommentierung, die sich in der Tiefe der Problemdurchdringung wie auch in Form der Durchdringung von Literatur und Rechtsprechung ausdrückt. Die Historie des Datenschutzes ist bei der Kommentierung präsent. Die bekannte Qualität des „BDSG-Simitis" wird gehalten. Insofern ist das Werk ein „Muss" für Leute, die sich mit Datenschutz wissenschaftlich befassen. Dies gilt praktisch durchgängig für alle AutorInnen, auch wenn sie sich in Stil und Materialbearbeitung unterscheiden. Der Abdruck der Erwägungsgründe und des Gesetzestextes, ein ausführliches Stichwortverzeichnis sowie ein aktuelles (auf die DSGVO sich beziehendes) Literaturverzeichnis runden die Nützlichkeit des Werkes ab.



Schwarze
EU-Kommentar
Becker, Ulrich/Hatje, Armin/Schoo, Johann/Schwarze, Jürgen (Hrsg.)
4. Aufl. 2019, ISBN 978-3-8487-3498-8, 3840 S., 259,00 €

(tw) Seit dem Jahr 2018, der direkten Anwendbarkeit der Datenschutz-Grundverordnung, hat das Europarecht für DatenschutzjuristInnen eine noch zentralere Funktion erlangt als bisher: Die Normen werden vorrangig nicht mehr vom Grundgesetz bestimmt, sondern von den Verträgen zur Europäischen Union (EU). Die Rechtsprechung wird nicht mehr vorrangig von Bundesverfassungsgericht geprägt, sondern vom Europäischen Gerichtshof (EuGH). Und der strukturelle, der organisatorische und prozedurale Rahmen der Gesetzgebung sowie der hoheitlichen Aufsicht wird nicht mehr nur von nationalen Behörden bestimmt, sondern auch durch europäische Gremien, Organe und Institutionen. War es also bisher für eine DatenschutzjuristIn üblich, zumindest einen Grundgesetzkommentar im Bücherschrank stehen zu haben, so muss künftig zumindest ein Grundsatzwerk zum EU-Recht verfügbar sein.

Um ein solches handelt es sich beim „Schwarze", der nun in 4. Auflage erschienen ist und mit knapp 4000 Seiten eine wahre Fundgrube zum aktuell geltenden europäischen Verfassungsrecht darstellt. „Verfassungsrecht" ist angesichts des weiterhin supranationalen Charakters der EU eine starke, aber berechtigte Bezeichnung: Der Schwarze liefert eine umfassende Kommentierung der gültigen Rechtsgrundlagen der EU-Verfasstheit, als da sind der „Vertrag über die Europäische Union in der Fassung des Vertrags von Lissabon (EUV), der „Vertrag über die ‚Arbeitsweise der Europäischen Union" (AEUV) und die „Charta der Grundrechte der Europäischen Union" (GRCh bzw. GRC).

Dieses für Normalmenschen nur noch schwer erfassbare Regelwerk zu erschließen, ist ohne fremde Hilfe auch für ExpertInnen praktisch nicht möglich angesichts der Masse an Verordnungen, Richtlinien und Beschlüssen der EU sowie der umfangreichen EuGH-Rechtsprechung, die von Portugal bis Finnland und Griechenland und damit auch für uns bestimmend ist. So begründet Art. 39 EUV die Zuständigkeit der EU für den Datenschutz, sichert die Überwachung durch „unabhängige Behörden" zu und verweist auf Art. 16 des AEUV, der neben einer ersten Grundrechtszusage die Zuständigkeiten des Parlaments und des Rats für den Erlass von Normen begründet. Die weitere Konkretisierung der Grundrechtszusage erfolgt dann in Art. 8 GRCh, der als weiterer Dreh- und Angelpunkt der weiteren Grundrechtskonkretisierung fungiert mit seinen Verweisen auf Zweckbindung, Einwilligungsgrundsatz und Betroffenen- insbesondere Auskunftsrechte.

Durch den Kommentar eröffnen sich – was von Fachleuten wie den DatenschutzexpertInnen leicht übersehen wird – die Bezüge des eigenen Bereichs zu anderen Lebens- und Regelungsbereichen, etwa den Schutz von ArbeitnehmerInnen und Verbraucherinnen, den Schutz vor Diskriminierung oder die Gewährleistung von Meinungsfreiheit und Demokratie. Nötig ist weiterhin die Einbindung des nationalen Regelungsrahmens in den größeren Rahmen der EU. Dies wird durch eine umfassende inhaltliche Darstellung, durch Verweise auf die relevante Rechtsprechung und Literatur sowie durch praxisnahe Darstellungen gewährleistet. Konsistenz, Vollständigkeit und Aktualität haben sich in der 4. Auflage weiter konsolidiert und können als zugesichert angesehen werden bei diesem grundlegenden Nachschlagewerk, das inhaltlich von nicht weniger als 47 einschlägigen AutorInnen bearbeitet wurde. Im Anhang werden die üblichen Verzeichnisse durch weitere generell relevante EU-Regelwerke (Protokolle und Verfahrensordnungen) ergänzt. Qualität ist schon immer etwas teurer gewesen; das Preis-Leistungsverhältnis ist aber hier kaum zu schlagen, weshalb die ca. 8 Zentimeter im Bücherschrank sinnvoll gefüllt sind.

Ein Russen-Hack?

Bei dem Prominentenhack hat sich herausgestellt, dass ein deutscher Hacker verantwortlich war. Vorab gab es die üblichen Spekulanten, die mit dem Finger auf die Russen gezeigt haben.

In geschlechtergerechter Sprache sind es „Russ*innen", „Russ_innen" oder meinetwegen „RussInnen"!

Wenn ich den Satz von Siri, Alexa oder Cortana in diesen Schreibweisen vorlesen lassen würde, käme „Russinnen" heraus. Gibt es demnach keine männlichen russischen Hacker mehr?

Es ist doch logisch, dass damit auch männliche Hacker gemeint sind!

